The Evolving Cyber Threat Landscape during the Coronavirus Crisis

CYBERDEFENSE REPORT

The Evolving Cyber Threat Landscape during the Coronavirus Crisis

Zürich, December 2020

Cyberdefense Project (CDP)
Center for Security Studies (CSS), ETH Zürich

CSS ETH Zürich

ETH zürich

Available online at: css.ethz.ch/en/publications/risk-and-resilience-reports.html

Author: Sean Cordey

ETH-CSS project management: Myriam Dunn Cavelty, Deputy for Research and Teaching; Benjamin Scharte, Head of the Risk and Resilience Team; Andreas Wenger, Director of the CSS.

Editor: Jakob Bund
Layout and graphics: Miriam Dahinden-Ganzoni

DOI: 10.3929/ethz-b-000458221

Table of Contents

Executive Summary

In light of the societal changes wrought by the coronavirus pandemic, this report aims to examine the impact this crisis had on the general cybersecurity landscape, notably in terms of the attack surface and exploitation opportunities; to investigate the changing and recurring patterns of adversarial behaviors; and to illustrate and provide an overview of how threats actors have leveraged said epidemic in Q1/Q2 2020.

Accordingly, this report highlights that the coronavirus pandemic has generated a set of remarkable and psycho-societal, technical, and logistical-economic circumstances upon which malicious actors have capitalized. These factors include:

1) an expanded socio-technical attack surface due to the greater use and dependency on services and applications for telework provided through digital infrastructure in general and cloud infrastructure in particular;
2) a psycho-informational environment characterized by anxiety, uncertainty, and high demand for information;
3) a nexus of economic and trade uncertainty/ disruption, emergency procurement processes, compounded by the wide availability of nefarious cyber tools.

Additionally, the analysis of coronavirus-related cyber threats has underlined that, despite some alarmist public reporting, some degree of continuity can be found, notably with respect to the dynamic nature and types of attacks observed, the types of threat actors, and the overall volume of certain cyber threats (e.g. phishing and malspam). Adversarial behavior has nonetheless changed and evolved in at least four important respects:

1) Many threat actors were directly affected by the pandemic and had to adapt their criminal business models, leading to a reduction in certain types of threats and an increase in others. This was also reflected in the grayware and darkweb marketplaces.
2) The scale, sophistication, and *modus operandi* of certain cyberattacks has increased or evolved. Coronavirus-related credential phishing and ransomware were among the most prolific threats in terms, with threat actors deploying evermore sophisticated ploys (e.g. double extortion, shorter reconnaissance requirements, more powerful and complex denial of service attacks) against larger targets. Increased cooperation between threat actors has also been recorded.
3) While all sectors have been targeted in some way or other, threat actors have increasingly shifted from individuals to the critical infrastructure sectors most affected and under pressure by the pandemic. Geographically, targeting focused on areas particularly affected by the pandemic following hotspots as the first wave of infections made its way around the world.
4) The motivations of state-sponsored actors have expanded to coronavirus-related espionage targeting healthcare and research infrastructure.

Lastly, the cyber threat landscape of Q1/Q2 2020 is characterized by heightened risks and a plethora of threats, from ransomware to credential phishing, and business email compromise.

While some qualification of threat perspectives has set in following an initial rise of blanket concern, ample opportunities for abuse and adaptation remain, especially as the “special” circumstances will endure. This report thus emphasizes the value of three key recommendations:

1. As economic pressure increases and cyber threats continue to grow and adapt, the importance of cybersecurity awareness-raising, capacity building, and communication to all stakeholders will be critical, not limited to but with a particular focus on authentication methods and basic cyber-hygiene.
2. Quality threat intelligence, information exchange, cooperation, and coordination between all stakeholders are critical for fostering a better understanding and more comprehensive perspective of the evolving cyber threat landscape, bringing institutional gaps into view, and fostering trust. The efforts and initiatives various stakeholders took in this direction during the first six months of the pandemic should therefore be continued as much as possible.
3. The accelerated digitization and expanded adoption of telework has brought the issues of remote and cloud security to the forefront of cybersecurity efforts. Besides all the security flaws and vulnerabilities linked to widely popular cloud-based applications, users and companies, especially SMEs, need to start addressing the issues around the

use of personal devices and configuration of remote access technologies.

Introduction

The coronavirus is not only a health hazard but also cause for worries in the digital domain. As the coronavirus pandemic has been ravaging the world for the past year, upending the livelihood of billions and transforming social and professional norms, malicious actors in cyberspace have jumped at the chance of exploiting this crisis and the unique circumstances it has created for their benefit. As the months went by, the cybersecurity community and a rising number of media outlets have been apt to report on new cyberattacks involving the coronavirus – and there were plenty. However, in the first half of 2020, the general media and private-sector reporting on these issues has been fraught with exaggerations of increased volume and novelty, leading to a general narrative that the cyber threat situation during the first two quarters of 2020 was without precedent (e.g. Arampatzis, 2020; Check Point Software Technologies, 2020a; Miller, 2020; Richardson and Mahle, 2020). While this is an appealing narrative – echoing that of the pandemic at large – its underpinnings need to be critically assessed before any definitive conclusion can be made.

Cyber threats – whether they include the exploitation of vulnerabilities in software and hardware or of the fear and lack of awareness of users or cyber-enabled disinformation – are by nature a dynamic phenomenon that reacts to the evolving analog and digital environments. This is even more true for an event of this magnitude, transformation potential, and global reach.

As a result, we would reasonably expect change and adaptation to occur on both ends of the cybersecurity/-defense spectrum – i.e. attackers and defenders. In the case of adversarial behavior (the focus of this report), this could concern the issues of targets, motivations or the *modus operandi* of malicious actors. This is likely to be particularly true as the pandemic has fostered new opportunities for malicious actors as the attack surface increased – notably due to the move toward telework and the climate of fear and uncertainty surrounding the pandemic. These "opportunities" are principally linked to socio--technical changes and not any radical technical innovation or transformation, meaning that we should expect relative continuity in terms of the techniques and tools used for these attacks. Adaptation should, however, be expected in terms of how the malicious actors leveraged the crisis for their cyberattacks.

Analyzing the extent to which this hypothesis and expectations are true and are reflected in qualitative and quantitative analysis of the data – while acknowledging its incomplete and anecdotal nature – is thus the underlying goal of this report. The more specific aims of this report are threefold:

First, it aims to examine the impact the coronavirus epidemic has had on the general cybersecurity landscape, notably in terms of the attack surface and exploitation opportunities. Second, this study aims at shedding some light on both the changing and recurring patterns of adversarial behaviors in this space – in other words: changes and continuities. Third, to put things into perspective, it aims at illustrating and providing an overview of how the epidemic has been leveraged by threats actors.

Accordingly, the structure of this report reflects these overarching objectives. The first section, following an introductory section that sets the context and discusses how the pandemic has socio-technically affected the attack surface, discusses and highlights specific observed changes and continuities in adversarial behavior. In the second, more descriptive section, the landscape of coronavirus-related cyber threats is laid out. It provides a snapshot of the actors, their tactics, and their targets. While cyber-enabled influence operations have been of considerable importance and prevalence throughout this pandemic, this report focuses on "conventional" cyberattacks, such as phishing, distributed denial of service (DDoS) or business email compromise (BEC) attacks. The report then concludes by summing up the main findings alongside some open-ended thoughts with regard to preparations for future developments.

As a general disclaimer, this report was conducted based on open-source material only. This includes reporting from (mostly western) journalistic[1], commercial, specialized[2], governmental, and intergovernmental sources. Given the short time span between the events and this report, very little academic literature exists. Furthermore, due to the nature of the available reporting – which significantly depends on discovery, self-reporting, and economic interests of threat intelligence companies – threat observations generally do not cover all stakeholder groups and geographic areas to an equal extent. Lastly, due to the general challenges of recording cyberattacks (i.e. based on reporting and detection) that impede a complete accounting, incident rates and dates need to be viewed with an element of caution. These limitations notwithstanding, this report provides a broad overview of how attack surfaces and threat actor behavior have evolved during the first six months of 2020 (1 January to 30 June), and of the resulting security challenges.

[1] This includes, for instance, major technology newspapers or blogs, such as Krebs on Security, ZDNet or Schneier on Security.

[2] This includes, for instance, major security and technology vendors, such as Kaspersky, Proofpoint, Symantec (Broadcom), CrowdStrike, McAffee, Microsoft, CheckPoint Software Technologies, F-Secure, Cisco Talos, Google or Trend Micro.

1 Cyber Threat Landscape: Dynamics

The first six months following the outbreak of the coronavirus have been marked by adaptation. Students, workers, hospitals, schools, universities, governments, businesses large and small had to come to terms with a new socio-technical environment in the collective effort to bridge over the social and physical distances resulting from safety protocols. They were not the only ones. Cybercriminals and state-sponsored hacking groups (often referred to as advanced persistent threats (APTs)) have followed suit and adapted their attack patterns in an attempt to take advantage of the expanded attack surface linked to the increasing virtualization of social, economic, and political interactions. However, despite the various operational and behavioral changes, continuity, most notably in terms of threat actors, volume of cyberattacks and the techniques used, emerges as an underlying characteristic of the cyber threat landscape during that time-period.

The following paragraphs lay out these different dynamics in more detail: the first subsection (1.1) provides context as to the changing attack surface, outlining how these changes have provided new opportunities for abuse; the second subsection (1.2) describes some of the main resulting changes in adversarial behavior; the third subsection (1.3) underlines the general continuity of the dominant the cyber threat trends as they existed before the coronavirus outbreak.

1.1 Changes in the Attack Surface: Use of Technology and User Behavior

Over the past few years, cyberattacks and cyber operations have become more numerous and prevalent. A confluence of factors contributes to this phenomenon, including the increase in digitalization of our societies, the exacerbating geopolitical tension between states controlling formidable cyber capabilities that extends competition into the digital sphere, and the fragmentation of the Internet. These high-level developments receive reinforcement at the operational level from the speed, global reach, and the relative low cost and ease with which malicious cyber operations can be conducted. Combined with adversary assumptions about possible responses to their malicious actions, these defining features of cyber operations have led to perceptions of low risks of escalation and high potential reward, predicated on difficulties in the political attribution of attacks, and low costs of entry for both state-sponsored actors and criminals[3].

During the first six months of this pandemic, the same dynamics have generally persisted and can account – to some extent – for the continued intensity in cyberattacks. Coupled with these underlying factors, the pandemic has enhanced and created a new set of vulnerabilities, which expanded the exploitable attack surface leveraged by threat actors. Specifically, the working and communication realities brought on by the pandemic have significantly altered the use of certain technology, the behavior of users, and the economic-logistical environment. Put differently, the socio-technical, psychological-informational, logistical-economic changes wrought by the pandemic have created new opportunities for cyber threat actors.

1.1.1 Socio-technical Factors: Telework and Lockdowns Spurred Exploitable Technical and Behavioral Vulnerabilities

The first factor is socio-technical in nature and relates to the rapid transition towards remote work, the change in working procedures/habits, and the subsequently increase reliance of all layers of society on digital infrastructure and services. Together, these trends have not only expanded the attack surface but have also made adjusting organizations more vulnerable to both infiltration and exploitation.

Teleworking Infrastructure and Habits

Many organizations, from large governmental bodies to multinational businesses and small and medium enterprises (SMEs), have transitioned towards remote work – often in a rush to maintain business and operational continuity. In many cases, organizations lacked the time, preparation, plans, capabilities, cybersecurity awareness, or knowledge to do so effectively, risking to improperly set up these systems and make them vulnerable to attacks.

The unprecedented surge in remote work has led to an increase in Microsoft Remote Desktop Protocol (RDP) usage. The Internet indexing service Shodan reported a 41 per cent increase in the number of RDP endpoints available on the Internet in March (Shodan, 2020). The rapid proliferation of RDPs, however, made it harder for IT experts seeking to secure their organizations or institutions to identify unauthorized network connections, and thus offered hackers a chance blend in with legitimate traffic to gain access to internal networks (Mehrotra et al., 2020; Wiggen, 2020). Additionally, many of these RDPs – due to time and scaling constraints – were misconfigured and left exposed – at least 4.7 million as of the end of March (Aprozper, 2020; Cybersecurity & Infrastructure Security Agency and National Cyber Security Centre, 2020).

[3] Assessments in this vein are necessarily contextual and depend on the target and type of the cyberattack. An attack against a critical infrastructure would have a greater escalation potential than an isolated attack against a small business.

These two dynamics, coupled with renewed motivation and opportunity for such attacks, have resulted in an increase in RDP brute force attacks, with cybercrime groups usually putting captured RDP credentials up for sale on so-called "RDP shops" (Cimpanu, 2020a; Galov, 2020).

The increasing dependency on remote-access solutions and connections for operational continuity has also accentuated the potential (economic and business) impact of DDoS attacks against RDPs and virtual private networks (VPNs). These developments also help explain the re-emergence of extortion DDoS as well as the various attacks meant to overwhelm Internet Service Providers (ISPs) (Hope, 2020a; Nexusguard, 2020; Zurier, 2020). Indeed, the massive increase and redistribution of bandwidths for remote work has led to a decrease in bandwidths available to defend against DDoS attacks, which now have a stronger potential to cause disruption and downtime. These issues can be mitigated by a variety of techniques but need a level of planning and preparedness that many organizations, most notably SMEs, did not readily have at their disposal (iDefense, 2020).

***

As an aside, it is worth noting that national lockdown measures were top-down decisions imposed by governments, granting companies little control and foresight on the timeline to comply with these measures. This dynamic highlights the influence of emergency trade-offs and the need to find a time-sensitive way to balance concerns of health security and cybersecurity that allow for the reduction of potential tension between efforts to protect employees from health risks and to slow down infection rates by moving employees quickly into remote office and ensuring the security of the technology that would need to enable this new working mode.

In response, many in the cybersecurity community have sought to counterbalance this sudden tilt toward health security by increasing their services, funding, and attention towards the (not-so-new) risks and vulnerabilities of these technologies. For instance, some specialized (inter-)governmental agencies (e.g. the UK National Cyber Security Center, Singapore's Cyber Security Agency or the US Cybersecurity and Infrastructure Security Agency (CISA)), private companies (e.g. KPMG, E&Y, McKinsey, PwC), and cybersecurity community organizations (e.g. the European Cyber Security Organisation (ECSO)) published dedicated best-practice guides, standards, and alerts to raise cybersecurity awareness about the types of cyberattacks and ways of protecting oneself online during this pandemic. Among these, some dedicated guides were explicitly devised for SMEs (e.g. by the Scottish government, the EU Agency for Cybersecurity (ENISA), and the European Digital SME Alliance) and for the healthcare sector (e.g. ENISA).

In addition, some governments, including in the UK, have provided dedicated funding to boost cybersecurity (e.g. for training and certification) for sectors under particular duress, such as healthcare (Gov UK, 2020). Another important measure was the creation of "COVID-19 cybersecurity response packages" by different cybersecurity communities. One notable example is the "Cyber Solidarity Campaign", launched by ECSO and its partners, which gave free access to a package of national and international tools, insights, and expertise (ECSO, 2020). Similarly, the International Telecommunication Union's (ITU) initiative CYB4COVID was set up as a one-stop shop to provide a repository for many of these resources.

***

In addition to the security risks linked to the use of RDPs and some negligence in their setting up, the shift to remote office has also entailed that many IT systems lost their institutionalized protections. Indeed, many workplaces usually benefit from IT personnel tasked with the protection of internal networks, detection of threats, and regular patching of software (Wiggen, 2020). Compared to this infrastructure, private IT devices, such as phones and computers, and home networks are often less well secured, encrypted, and updated. Indeed, privately used computers often lack professional antivirus protection programs or firewalls and can run software that can have severe (unpatched) security gaps – either because of the quality of the software, lack of cyber hygiene on the part of the user, or products having reached the end of their support cycle (Wiggen, 2020).

To compensate for these shortcomings, many companies provided its workers with up-to-date (e.g. with encryption or firewall) work computers, dedicated VPNs, and teleworking tools. Some also reinforced their IT support for troubleshooting and explaining these new tools, which were new for many employees. However, many organizations did not or were not able to do so, whether for financial or practical reasons. As a result, many employees did end up using their own devices. According to a survey commissioned by the cybersecurity firm CrowdStrike, which interviewed 4000 senior decision-makers in various countries[4], 60 per cent of the respondents reported that they were using their personal devices to complete work (Sentonas, 2020). The same survey also revealed that a majority of companies (53 per cent) did not provide any additional cybersecurity training on the risks associated with remote work. This was particularly the case for SMEs, where 69 per cent of respondents reported to have received no additional cybersecurity training (Sentonas, 2020). A recent study has highlighted a similar trend for

[4] CrowdStrike commissioned YouGov PLC to conduct an online survey of 4048 senior decision-makers in Australia, France, Germany, Great Britain, India, Japan, Netherlands, Singapore and the US. Fieldwork was undertaken in the period 14-29 April 2020.

Swiss SMEs (Vifian et al., 2020). Awareness challenges contributed to these technical risk factors. A large majority of the respondents (89 per cent) were optimistic about their personal devices' cybersecurity and readily downloaded sensitive data on their personal devices. A significant share – around one in three in the UK – are not concerned about cybersecurity at all (Coker, 2020). Other surveys, notably by the VPN company Twingate and technology firm IBM, tend to support these general trends (IBM, 2020; Twingate, 2020).

Not all industries, however, have shifted to home office – with the subsequent loss of protection – in the same way. In Switzerland for instance, Deloitte conducted a similar survey with over 1500 respondents across different industries. While some results are very similar to those reported by CrowdStrike, the Deloitte survey highlighted that the public sector had difficulties (or more reticence) to transition to home office compared to other industries. According to the survey, 65 per cent of the workforce in the ICT sector worked completely from home, 50 per cent in finance and insurance sectors whilst only 25 per cent on average for the public sector[5] (Deloitte, 2020). Among the different difficulties, one finds the lack of technical support, delays in hardware delivery, and incompatible software (e.g. to access data). Indeed, only 29 per cent of employees working within administrations surveyed said that their employers immediately offered the technical support needed to enable them to work from home during the pandemic (Deloitte, 2020). Meanwhile, a significant majority of the civil servants surveyed (71 per cent) expressed frustration because the technical equipment to enable them to work from home took several days or even weeks to arrive or was never delivered at all (Deloitte, 2020). Finally, 58 per cent of civil servants surveyed said they did not have the right software to access data (Deloitte, 2020). In addition to the disruption caused to the usual work process and attention that could be leveraged by threat actors, the shift to home office in the public sector has for the most part been underlined with concerns around the issue of protecting sensitive and confidential data and the related risk of cyberespionage. In particular, the rapid reliance on third party/private software, tools and platforms for virtual collaboration and digital exchange reinforced the risks of data leaks.

Emblematic of the pandemic and the "new normal," remote work for most organizations implicated a shift towards teleworking technologies, such as the cloud-based conferencing tools Zoom or Microsoft Teams (see figure 1) and VPNs (see section 2.2.1). These technologies and their large-scale use, however, at the same time created high-value target sets that malicious actors tried to exploit, whether for criminal purposes or for economically or politically motivated espionage. By way of example, it is worth recalling that early on in this crisis, the UK's cabinet held meetings through Zoom (Cybersecurity & Infrastructure Security Agency and National Cyber Security Centre, 2020; McAfee, 2020a). However, many of these teleworking technologies suffered from security vulnerabilities – sometimes due to coding errors, misleading claims (e.g. about encryption), or rushed expansion of their services. Malicious actors have actively sought and sold such vulnerabilities on the dark web. Their widespread – and relatively new – usage (and thus potential reward) made these particular technologies prominent targets of cyberattacks, such as credential stealing, phishing, and brute force attacks (see section 2.2.1).

Figure 1: Increase in the usage of teleworking technologies - January to mid-March (McAfee, 2020a)

In addition to the technical vulnerabilities it has created or enhanced, the shift to telework also affected various organizational procedures and work/life habits, contributing to an expanded attack surface and exposure to malicious activity – notably scams and business email compromise. Among these, several factors have helped criminals harvest details or divert millions of dollars from government and companies (Interpol, 2020a). One factor was that to protect the health of their workers and address the urgent need for protective material, many organizations waived the normal procurement controls and dealt with new, unknown – and sometimes untrustworthy – suppliers. This considerably reduced controls and possible detection of scams, while the considerable amount of money spent on these orders only added to the attraction for cybercriminals. As a side effect, travel and lockdown restrictions complicated face-to-face meetings between customers and suppliers (The Economist, 2020). Communication and agreements had

[5] A more detailed breakdown for the public sector shows teleworking of 33 per cent for thefederal level, 27 per cent for the cantonal level, and 15 per cent for the municipal level (Deloitte, 2020).

to be done and negotiated online, with reduced safeguards to verify identities that made it easier for malicious actors to insert themselves into and exploit the process.

Indeed, it offer a plausible explanation for some companies as to why payment details used during the pandemic differ from those on record for past transactions (Peterson, 2020). Faced with disruptions of global supply chains due to trade, workforce, and travel restrictions, competition for scarce resources put many companies under pressure to prove their financial commitment to their suppliers, resulting in less rigorous verification of invoices and payment requests (Peterson, 2020).

In addition, teleworking has dramatically increased the volume of professional emails, leading — as a side effect – to "email/telework fatigue" and diminished attention to detail due to overload (Peterson, 2020). This can help explain the increased success rate of phishing, notably those using email as the attack vector (see section 2.2.4) (Lefferts, 2020). Additionally, this fatigue, coupled with the psychological and economic factors, has made business email compromise (BEC) particularly effective, notably when malicious actors use a coronavirus framing (for an in-depth discussion of the use of BEC see section 2.2.6).

Mobile Devices and Social Media

Smartphones are now ubiquitous in most regions of the world. In many countries, they are even more prevalent than computers. Mobile devices play a central role in the way we socialize, inform, and entertain ourselves. This has been even more the case during this pandemic, where people have been separated from their friends, families and colleagues, and have been longing for both information and entertainment. As for telework, the pandemic has also altered or reinforced some user habits concerning mobile technologies – dynamics that played into and exacerbated threats.

The pandemic has greatly increased this reliance and the time users have spent on their phones and other digital media. A growing body of literature supports this trend across a variety of populations. A study of 254 Canadian families with young children reported an increase of screen time for mothers, fathers, and children during COVID-19 by 74 per cent, 61 per cent, and 87 per cent, respectively (Caroll et al., 2020). Moreover, a study conducted in China found that about 70 per cent of 1033 participants spent more time looking at screens after the COVID-19 outbreak (Hu et al., 2020). Another study recruited 4108 participants from nine European countries and found a 65 per cent increase in screen time among the participants during this pandemic (Pišot et al., 2020).

Linked to this general trend, one finds a corollary – albeit not direct – increase in the reliance on and usage of social media – with a particular emphasis on video-based, gaming and live-streaming apps and features. More generally, the number of social media users has grown by more than 12 per cent compared to last year – slightly over the 9 per cent trend of 2018 and 2019 – taking the global total to approximately 3.96 billion by the start of July, according to digital reporting company DataReportal[6] (Kemp, 2020). More specifically, while there is a general trend toward increased usage, it varies across countries and has been driven by other factors not related to the coronavirus, such as for instance the US elections. For instance, in the US, the Harris Poll reported that in March and May, between 46 to 51 per cent of American adults were using social media more frequently than before the outbreak (Samet, 2020). In Switzerland, by contrast, social media use has intensified for only around a quarter of the surveyed population[7] according to a survey run by researchers at the University of Zurich (Hargittai and Nguyen, 2020).

Despite the various measures taken by social media companies, the increased engagement on these platforms has played a key role in the nefarious development and spread of mis- and disinformation related to the pandemic (see next subsection for more details on the "infodemic") – a dynamic that has played into the climate of fear and uncertainty exploited by malicious actors. This is particularly illustrated and spurred on by the fact that a considerable number of people now read and share their news on social media. While there is no definitive number worldwide, in Switzerland, over 70 per cent of the individuals surveyed obtained information on the coronavirus through one of the main social media platforms (i.e. WhatsApp, Facebook, Instagram, twitter and YouTube) (Hargittai and Nguyen, 2020).

Apart from the public health concerns linked to the rising screen time (e.g. for mental health and lack of physical activity), the main concern from a cybersecurity perspective is that of an increased exposure to malicious material, be it disinformation or malware, coupled with a renewed interest from malicious actors to exploit the situation. Indeed, contrary to computers and IT networks, mobile cybersecurity hygiene is less mature and less well-integrated into people's minds. These "pocket-sized computers" also suffer from less institutionalized protection and available cybersecurity solutions while collecting and storing a trove of sensitive

[6] According to the latest report from DataReportal, there has been an important acceleration between the months of July and September 2020 – illustrating a certain acceleration of the phenomenon that can be linked to habits developed during Covid-19 lockdowns (2020).

[7] The survey was conducted in mid-April. It involved 1,350 individuals across the 26 cantons.

personal and financial data (Dawson et al., 2016; Kaspersky, 2020; Winder, 2019).

Over the last few years, cyber threat actors have wasted no time and efforts exploiting the attack surface offered by smartphones and have continued to do so throughout the pandemic. Examples of such cases include the different malicious apps that were developed to capitalize on the increased information demand and change in working behaviors (e.g. fake COVID-19 tracking map or contact-tracing apps, malicious apps posing as Zoom variants, fake symptoms check app). Among the most common threats, we find banking Trojans, scams, and ransomware (see section 2.2.2).

***

The resulting combination of an increased attack surface coupled with a reduction in IT defenses and oversight capabilities has resulted in an overall increase in the risk of becoming a target of cybercrime, cyberespionage, and cyber-enabled disruption (Fidler, 2020). Cyber threat actors have readily identified these susceptibilities and vulnerabilities and have targeted the most popular services and devices for telework: email, texting/SMS, video calls, conference calls, VPNs, and home networks (Intsights, 2020). As shown in the following sections, threat actors have also adapted their attacks to the new environment. Fear, need for information, and curiosity have been particularly targeted at the level of individual users. At the company level, time constraints and financial pressure have been among the key factors malicious actors have sought to leverage in their favor.

1.1.2 Psychological and Informational Factors: Fear and Uncertainty Spurred Demand for Information

The second factor that influenced the coronavirus-related cyber threat landscape has been the psychological impact of the pandemic. The crisis has fostered an environment characterized by widespread anxiety, insecurity, uncertainty, and fear (Peterson, 2020). An environment that all types of cyber threat actors have opportunistically and creatively exploited, whether in their scams, fraud, and extortion (see section 2.2.3), phishing and social engineering (see section 2.2.4), fake coronavirus-related apps (see section 2.2.2), spam attacks (see 2.2.7) or business email compromise (see section 2.2.6).

Interestingly, reports – notably from the technology firm Microsoft – have indicated a spike in the success of such attacks, especially for social engineering (Lefferts, 2020). This success/trend can be explained by the fact that when someone's health is involved, the need for information or curiosity can be easily aroused – and thus abused (Mouton & de Coning, 2020). Moreover, strong emotions can often take precedent over suspicion and beat critical thinking, leading users to blindly follow instructions, especially when coming from seemingly credible and recognizable sources (SingCERT, 2020). This last element has been particularly prevalent and key as official communications from governments, schools, or employers were expected by individuals. Knowing so, threat actors have readily and craftily imitated such sources to conduct their schemes.

In addition to spoofing, social engineering and phishing attacks have sought to leverage hoaxes and conspiracy theories or mixed fabricated with authentic information to arouse interest. As a result, purposely or opportunistically, cyber threat actors have contributed and reinforced the environment of anxiety as well as the "infodemic"[8] that has plagued the coronavirus response. This dynamic has also been a central accelerating factor for the number and success of these cyberattacks (CyberPeace Institute, 2020).

The intensified need for information by policymakers, companies, and individuals at the center of this "infodemic" has been coupled with a relative uncertainty of the information and data available; a discrepancy that allowed threat actors to thrive by presenting and playing different narratives and facts off against each other. Policymakers, in particular, were in need of reliable data to devise effective public health and economic responses. Many, however, have operated with inadequate information – most notably linked to the medical and scientific uncertainty around the virus (Canadian Center for Cybersecurity, 2020). This dynamic was reinforced by the relatively limited time to consume information coupled with the scarcity of reliable data. The relative abundance of information sources and information channels on the other hand has complicated the sourcing and potentially the verification of certain claims and data points.

The "infodemic" and climate of fear is not only linked to uncertain data and inadvertent misinformation but also targeted and mass-scale deliberate disinformation. Malicious actors – notably those backed by states – have leveraged this need for specific information to advance some of their strategic aims (see section 2.1). These ambitions include advancing specific narratives or sawing conflict, disruption, division, and dissent around the pandemic and its response (Intsights, 2020). Examples include the disinformation campaign around martial law being declared in the US and the UK and fabricated speculation about the virus originating from the US (Associated Press, 2020).

[8] Understood as an excessive amount of information about a problem that is typically unreliable, spreads rapidly, and makes a solution more difficult to achieve (Oxford Dictionary, n/a).

Lastly, the need for intelligence – notably on the spread of the disease, its impact on state rivals, and vaccine research – has also driven intrusion campaigns against medical organizations and research facilities by criminal and state-sponsored actors (see section 2.1). These actors have readily exploited the existing – and well-documented – socio-technical vulnerabilities in this sector but also the exacerbated time and resource pressure under which these institutions had to function during the pandemic.

1.1.3 Economic and Logistical Factors: Economic Uncertainty, Availability of Grayware and High Demand for Certain Goods Enabled Cybercrime

The third set of factors relates to different economic dynamics, namely those unfolding on financial markets and on grayware/malware markets, as well as the disruptions to trade and the global flow of goods.

The pandemic has already led to a global economic downturn, leading to a rise in unemployment and a subsequent increase in poverty, economic uncertainty and distress. In the US, for instance, unemployment has risen to 13 per cent (US Bureau of Labor Statistics, 2020), while in OECD countries rates increased to approximately 8.3 per cent for Q2 2020 (OECD, 2020). A network of factors including the loss of revenue, an increase in available time, and a decrease in mobility has led to a rise in the number of actors engaged in cybercrime as a source of income.

Governmental responses to income uncertainty, by way of distributed and massive financial aid and economic stimulus packages – e.g. two trillion USD in the US and 750 billion EUR in the EU – have also attracted a number of cyber threat actors. The form in which some of these funds have been dispersed – e.g. as risk-free loans managed by banks and other financial institutions – only added to the risk profile of these institutions and the pressure of expectations for providing quick relief they experienced (Najarian, 2020).

Moreover, market volatility and interest rate cuts have also been creating conditions and an environment that can be leveraged by fraudsters and scammers. With investment markets plunging in the first half of 2020, and certain central banks cutting the base rate (e.g. Bank of England or the US Federal Reserve), pension and investment customers and savers have been tempted to withdraw or transfer money from their plans to stanch short-term losses or generate some income. Cybercriminals have readily exploited concerns about the security of savings, investments, and pensions by luring victims into fake early access to pension funds or investment scams (Zurich, 2020).

In addition to income and financial uncertainty, the inadvertent disruption to trade, logistics, and production caused by restrictions that were put in place to mitigate the spread of the virus have also fostered a high demand for certain goods, including both specialized equipment (e.g. protective gear) and every-day items (e.g. toilet paper). This demand, in turn, has created new opportunities for abuse by cyber threat actors, be it for goods-based scams, phishing, or malspam (see section 2.2.3, 2.2.4 and 2.2.7).

These logistical elements are rooted in several developments and dynamics. Disrupted production and trade lines contributed to shortages or limited availability of certain products, notably protective gear. Such sought-after products have been a common subject of scams. The shortages in protective gear were accentuated first and foremost by limited international production capacity and willingness to export any stocks that followed Chinese efforts to buy up global supplies in the early stages of the pandemic. In January and February, Chinese exports of these goods contracted about 15 per cent while its imports were about 47 per cent of global production. China's exports gradually increased in later months – recording a 338 per cent increase by April – facilitating supply of protective gear to the most affected countries (UNCTAD, 2020).

The spread of mis- and disinformation around the pandemic, coupled with a climate of anxiety, has also been a key factor contributing to the scarcity of certain products. Panic and opportunism has fueled bulk buying and price gouging. In addition, the closure of national borders and subsequent tight control and confiscation of "critical medical assets" intended for export – including protective gear or test kit components – further heightened concerns about shortages and the urgency to secure supplies, including through unconventional channels.

In parallel, this growth in the number of cybercriminals has been supported and enhanced by the accessibility provided by flourishing underground markets and platforms for cybercrime tools (e.g. phishing templates or ready-to-run malware) and cybercrime-as-a-service. Indeed, the emergence of the grayware market and the increased commercialization of keyloggers, stealers, and Remote Access Trojans (RATs) has only magnified the various threats by reducing the barrier to entry for attackers, even those with limited programming skills or computer science expertise (Brumaghin and Unterbrink, 2020; Interpol, 2020a).

Anecdotally, analysts from the threat intelligence firm iDefense reported in April a significant increase in the sale of the popular Android banking Trojan *Cerberus* on criminal underground forums (e.g. XSS, Exploit and Club2crd (iDefense, 2020). Notably, the premier seller of the malware claimed to have sold more in one week than in the previous four months combined (iDefense, 2020).

1.2 Changes in Adversarial Behavior: Adaptation of *Modus Operandi* and Targeting

Cyber threat actors have utilized the pandemic in a myriad of ways. Many reports and observers have described or portrayed these threats as unprecedented. While the extent to which these threats are unprecedented warrants a critical assessment (see section 1.3), it would be reductive to argue that the behavior of cyber adversaries has not been affected by the pandemic. Accordingly, the following paragraphs highlight four of these key changes.

1.2.1 Cybercrime Business Model

The first change has revolved around the business models of many cybercriminals. Indeed, underground and Darkweb hacking forums and grayware markets have reacted and adapted at a greater scale and speed than usual. Early on, many of these platforms adapted their offers and tailored them specifically for coronavirus-themed attacks (Europol, 2020a; Intsights, 2020). For instance, scams and phishing templates (e.g. for specific governments or the World Health Organization (WHO) have proliferated, adapting to the new demands and consumer habits brought on by the pandemic (e.g. in masks, toilet paper, ventilators, and thermometers) (Trend Micro, 2020a).

Furthermore, while many cybercriminals seem to have thrived, the outbreak has also acted as a double-edged sword for many others, who saw their business models collapse (Afifi-Sabet, 2020). Reports have shown that many cybercriminals have expressed their worry and desperation as to how the pandemic had affected their established business models. As a result, many have urgently tried to adapt their activities to the changed landscape (Afifi-Sabet, 2020; Guirakhoo, 2020a). Mirroring offline life effects of the pandemic, some of the most affected malicious actors were the ones that specialized in various aspect of work life such as travel or events severely constrained by the pandemic. These saw their revenues dry up nearly overnight as lockdown measures were imposed across the world (Afifi-Sabet, 2020).

Related to this, cybercriminals engaged in bank fraud, cashing out and warehouse/bank drops[9] saw their activities considerably slowed down and disrupted for the same reasons (Photon Research Team, 2020). The daily activities of money mules have been disrupted in a number of countries – e.g. Spain, Italy – as they were afraid or unable to leave their homes (Intel471, 2020). Reshipping mules, which usually pick up diverted goods in hotel lobbies or shops to stay anonymous, also saw their operation disrupted because of the social distancing norms in addition to the increasing wait time when calling FedEx, UPS or banks in general (Krebs, 2020a). In addition, Amazon and other global providers blocked shipments of non-essential and often more expensive products, thus considerably limiting the range of available goods for such scams.

The pandemic has paved the road for wayward attempts at self-styled charity in the world of cybercrime. Several cybercrime vendors have launched promotion and marketing campaigns for their hacking services or malicious tools offering special "COVID-19" discounts and giveaways, allegedly to support "financially struggling" customers. One example includes Brian's Club — one of the underground's largest bazaars that sells stolen credit card data — which began offering "pandemic support" in the form of discounts for its most loyal customers (Krebs, 2020a). While giveaways, free advice, and donations have been part of the underground scene for a while, the offers related to coronavirus exploits and the appeal to the emotional and financial distress in order to attract new customers, such as amateur cybercriminals, is new. One of the main motivations behind these offers and discounts is the bid by these vendors to increase their reputation and credibility (Photon Research team, 2020).

***

These changes illustrate the inherent dynamic and adaptability of threat actors. While the abovementioned specific cybercrime models were highly disrupted during the first six months of the pandemic – and continue to be so in many regions – they are nonetheless expected to return in some form or other once economic life in affected sectors recovers. In the meantime, other types of threats were created to leverage the pandemic in each of its different phases. This dynamic will only continue and the threats will only proliferate. The knowledge, technical gains and innovation achieved during the pandemic, however, will continue to show their effects in the years to come.

1.2.2 Scale, Sophistication, and *Modus Operandi* of Cyberattacks

The second change observed has been a shift in the scale of some types of attacks, the nature/sophistication of cyberattacks, and the *modus operandi* of different threat actors.

Among these, one pre-eminent change has been in the scale[10] of some campaigns, most notably

[9] This term refers to the individuals employed to visit banks to withdraw money from fraudulently acquired accounts, allowing cybercriminals to "cash out" their illicitly earned funds.

[10] As a caveat and premise to section 1.3; despite the increase in scale of phishing attacks, the general scale and volume of malware and cyberattacks has remained consistent over time (Microsoft, 2020).

coronavirus-themed phishing attempts. This increase in scale can be explained by the aforementioned set of psycho-informational factors and the opportunistic and geopolitical logic inherent to the different malicious actors. This willingness of grasping the opportunity presented by the pandemic is apparent in efforts during the early months of the pandemic, when cybercriminals actively recruited collaborators – e.g. amateurs or former money mules – to orchestrate these large-scale phishing campaigns and maximize the impact of their attacks (Europol, 2020a).

Another observation is that the complexity and sophistication of the attacks have evolved compared to the previous year and as the pandemic progressed and hit different parts of the world. For instance, the initial phishing and malware attacks in the early months of the year – before the pandemic reached Europe – were relatively simple. However, they grew in sophistication, with better coordination and improved lures (i.e. templates, websites, etc.) as they began to target increasingly more complex organizations (e.g. governments, or hospitals). In addition, Microsoft posits that attackers, particularly state-sponsored ones, have also become more sophisticated in performing reconnaissance on high-value targets, reflected in considerations of factors like public holidays that might reduce the victim organization's ability of responding in real-time, or otherwise hardening their networks (Burt, 2020). Criminals, meanwhile, are also now following even more holistic strategies by notably employing and exploiting a greater variety of tools, systems, and vulnerabilities, including by assuming false identities and through close cooperating with other groups (Europol, 2020b).

Another change pertains to the *modus operandi* associated with certain types of cyberattacks; some of which have changed while certain cyberattacks have been preferred to others. For instance, cyberattacks such as reshipping attacks or scams involving non-essentials products have seen far less windfall profits from the pandemic compared to other criminal activity due to operational difficulties. By contrast, credential stealing via phishing attacks and ransomware have become among the most prevalent types of attacks, greatly benefiting from the socio-technical vulnerabilities fostered by the pandemic. According to Microsoft, many cybercriminals have readily leveraged the pandemic context and shifted their focus to phishing attacks – amounting to approximately 70 per cent of the attacks observed – as a more direct means to achieve their goal of harvesting credentials (Microsoft, 2020). As illustrated in section 2.2.4, attackers have often sent emails imitating top brands (e.g. Zoom, Microsoft, UPS, Amazon, and Apple among others) and official organizations (e.g. CDCs, health agencies, or tax and revenues agencies).

In combination with the opportunistic and profit-maximizing logic that underlines these attacks, cybercriminals have tweaked their attack methods, notably for ransomware. According to Europol and Microsoft, cybercriminals have shortened the period between the initial infection and the activation of the ransomware attack, thus not waiting for an ideal moment to launch the attack but trying as soon as possible to cash in (Europol, 2020c; Muncaster, 2020a). In some instances, cyber-criminals went from initial entry to holding an organization's entire network for ransom in under 45 minutes. Furthermore, since the beginning of the pandemic, malicious actors seem to have widely adopted a new form of ransomware attacks for double extortion. In this scenario, the attackers exfiltrate large quantities of data prior to encrypting it. Victims who refuse to pay the ransom are threatened with the data being leaked or sold on the black market, putting additional pressure on them to meet the criminals' demands (Check Point Software Technologies, 2020a; MELANI, 2020). In addition to the *Maze* ransomware, *Sodinokibi/REvil*, *DoppelPaymer*, *Mespinoza/PYSA*, *NetWalker*, *CLoP*, *RagnarLock*, and *Nefilim* have also been observed using this technique (Coveware, 2020).

Malicious actors have also taken advantage of people spending more time at home and the related increase in online activity (i.e. online shopping) to engage in online carding activities. Due to the increased amount of online banking transactions – e.g. in March online operations made up more than 50 per cent of banking transaction compared to the usual 33 per cent – carding fraud has become more difficult to attribute and to detect (Photon Research Team, 2020).

Another evolution has been around mobile threats. Throughout the early months of 2020, threat actors have been seeking new infection vectors in the mobile world, changing and improving their techniques to avoid detection in places such as the official application stores. In one innovative attack, threat actors used a large international corporation's mobile device management system to distribute malware to more than 75 per cent of its managed mobile devices (Check Point Software Technologies, 2020a).

1.2.3 Targets

is the pandemic has shaped a distinct pattern of the geographical distribution of cyberattacks, as well as for the way and intensity with which some victims have been targeted by malicious actors.

Unsurprisingly, cyberattacks during the coronavirus pandemic have followed a logic of opportunism and have intensively targeted countries that were the most affected by the virus. Reports in March and April, for instance, highlighted spikes in coronavirus-related cyberattacks in Italy, Spain, France, India, the UK, the US, and Canada (Arsene, 2020a; F and

Scholten, 2020). Meanwhile, states such as China and Japan that were affected earlier in the year also suffered coronavirus-related cyberattacks ahead of other countries.

In terms of targets, one major change during these first two quarters of 2020 has been the relatively novel and intense targeting of the healthcare sector (alongside the education sector) for both profit and espionage.[11] Attacks against the healthcare sector as such are far from new and have been relatively easy and common as healthcare providers are acutely vulnerable not only to social engineering schemes but also to relatively unsophisticated attacks (e.g. RDP brute force) because of the use of unsupported operating systems or misconfigured web servers (Microsoft Threat Protection Intelligence Team, 2020; Schneier and Bourdeaux, 2020). In the past years, there has been a considerable number of – direct and indirect – ransomware attacks against such organizations. From mid-2018 to mid-2019, Recorded Future catalogued 134 publicly reported ransomware attacks against healthcare providers in the US (Liska, 2020a).

The novelty here is the increased criticality of these organizations and the stress under which they operate due to the pandemic. These factors, compounded by the often inadequate cybersecurity resources and the opportunist and strategic logic of some malicious actors, has led to an increase in intensity and systematization of attacks against them (see section 2.2.8). Just to illustrate, the WHO saw a 500 per cent increase in cyberattacks against its systems (WHO, 2020a).

As such, the targeting of the healthcare sector is part of a greater trend identified by Interpol where malicious actors, particularly cybercriminals, driven by a profit-maximizing logic, have shifted from individuals and small businesses to major corporations, governments and critical infrastructure – including major IT companies and financial providers such as Cognizant or Finastra (Interpol, 2020b). The substantiveness of this assessed shift is difficult to fully verify, but the increase in exploitation of remote-working tools and infrastructure could be a hint in that direction. In addition, disruptive and information-stealing malware attacks seem to have focused on larger organizations due to the higher potential rewards. Nonetheless, individuals and small businesses that mostly operate online remained, at least in the early stages of the pandemic, an important target group (Krebs, 2020a).

Another important trend relates to cloud-based services and teleworking infrastructure and data, which have also been increasingly targeted – as companies, schools, and governments moved online, which at the same time facilitated their exploitation by threat actors. Microsoft shared that in some regions the growth in its cloud service increased by as much as 775 per cent during March,[12] a rise that has since normalized (Microsoft Azure, 2020). Usage of cloud services has increased by approximately 50 per cent compared to January, with manufacturing and financial services leading the way, whereas online video conferencing services specifically saw an increase in usage of up to 600 per cent compared to the beginning of the year, mostly driven by the education, governmental, and financial sectors (McAfee, 2020a).

Concurrently, McAfee saw the number of external cyberattacks[13] against these infrastructure and services – particularly exploiting Office365 – increase by 630 per cent between January and April 2020 (McAfee, 2020a).[14] Accordingly, malicious actors have readily exploited and attacked cloud infrastructure vulnerabilities (e.g. one critical vulnerability in Microsoft Azure discovered in January), cloud service providers drawing on misconfigurations and user errors (Check Point Software Technologies, 2020b).

On top of that, threat actors are also using cloud infrastructure to their advantage and have increasingly started to store and disguise the malicious payloads used for their malware attacks in the cloud (Check Point Software Technologies, 2020b). Threat actors have disguised and stored malicious payloads on GitHub, Gmail or Alibaba to deliver commands or host configuration files. In other cases, just uploading seemingly benign documents with malicious links to Google Drive can give them the extra touch of legitimacy needed to trick unsuspecting victims. Cloud services are aware of these activities, but threat actors are adapting with encryption and camouflage techniques, offering droppers dedicated to placing malware on the cloud (Check Point Software Technologies, 2020b).

1.2.4 Motivation of State-Sponsored Actors

A last change has been the motivations and objectives of many state-related threat actors. During these first six months of 2020, the objectives of these malicious actors seem to have largely been framed by one theme, namely the pandemic and its response. This has translated into organized, and coordinated efforts towards intelligence collection and espionage on vaccine and treatment

[11] In the later quarters, this trend seems to have diminished but is expected to rise again with new waves of infections.

[12] More specifically, this statistic refers to the number of monthly users in Italy organizing online meetings and coals through Microsoft Teams. Italy had rigorous social distancing or shelter in place orders in force during that period.

[13] Indicated either by excessive usage from new locations or suspicious behavior that deviates from patters observed for human users.

[14] In February, the rate of cloud attacks was higher than the increase in adoption of cloud services. Between March and April, however, the two seem to have evolved linearly (McAfee, 2020a).

research and other types of strategic data related to the pandemic (e.g. infection rates). This also includes information regarding the coronavirus pandemic's effect on military preparedness. These espionage dynamics have not only been driven by but have also fostered increasing international tension and competition, both between adversaries and like-minded states.

Such information is of critical strategic value for all affected states as it would provide key strategic health, economic, and political benefits for fighting the pandemic, returning to "normalcy" and limit the economic ravage that prolonged lockdowns, social-distancing measures, and the looming recession have brought. In addition, vaccine espionage is undertaken in a climate of geopolitical rivalries underlined with fears that even following the discovery and approval of vaccines, their availability and distribution might be tied to political or economic conditions. These concerns remain despite the tentative reassurances made by most states to make the vaccine a global public good.

Consequently, and as mentioned above, institutions and organizations of the healthcare sector, the pharmaceutical and biotechnology industries, government agencies monitoring these sectors as well as operators of logistic infrastructure involved in the distribution are moving into the crosshairs of intelligence services and APTs (Wiggen, 2020). An overview of the different cases reported is provided in section 2.1.2, but the general trend indicates a "free for all" where threat actors from across the world compete against one another for this intelligence, many of whom are using COVID-19 lures as this theme has proven to be a virtual opener for exploitation.

As a result, western national (cyber-)security bodies, such as NATO, the UK National Cyber Security Centre (NCSC), the Canadian Communication Security Establishment (CSE), or the US Cybersecurity Infrastructure Security Agency (CISA) and National Security Agency (NSA), and political leaders, such as the European Commission President von der Leyen, have explicitly warned of and linked some of these cyberattacks to Russian (i.e. APT29) and Chinese threat actors (National Cyber Security Centre, 2020a, 2020b; Stolton, 2020). Reports by the cybersecurity industry have corroborated such claims. These views are, however, far from representative, considering business-driven incentives to highlight risks and to focus on threats to well-paying customers. Most of the English-language public reporting by the cybersecurity industry is produced by western companies and may reflect a collection bias against US adversaries given the companies' customer base. Due to high-profile strategic interests at stake, it is highly likely that western states also engage in similar actions.

Notably, cyber-enabled industrial espionage against research institutions and healthcare is far from new. Both China and Iran have been known for hacking and exfiltrating intellectual property in order to catch up, retain or develop a strategic advantage in specific issue area (targeting, among others, military organizations, nuclear research, or the tech industry). Accordingly, it is these past experiences and the development of the necessary capabilities and infrastructure for these targeted attacks that help explain, in part, the prevalence and volume of these attacks, particularly by China and Iran.

As mentioned, these expanded motivations and attack dynamics have been fostered, in part, by the rising international tensions, particularly in the relations between the US and China but also between China and Australia. The Sino-American relationship, already tense since the trade war and the competition for 5G, has only deteriorated further as the pandemic developed. Causes include disinformation and propaganda on both sides, overt racism from the Trump administration, the removal of Hong Kong's special policy status, the mutual accusation of cooptation of the WHO, and the indictment of Chinese cybercriminals/spies. As a result, the increase in geopolitical competition and deteriorating dialogue between the United States and China will likely encourage higher profile attacks on telecommunications, technology, and finance firms, and critical infrastructure industry verticals in the US and allied countries (Clark, 2020).

This dynamic played into other crucial drivers, such as the demand for medical intelligence, particularly in a context where official data may not always be transparent or trustworthy. Indeed, the publicly released data of many states and bodies, such as Iran, China, the WHO and now the US have been heavily questioned. Many states have been accused of lying or not fully disclosing the full range of the spread of infections and the concomitant threat to public health. This dynamic was and is particularly reinforced in countries where the press is not free and where censorship on the issue took place.

Another contributing factor are the lockdowns, the limitation on international flights, and social-distancing norms, which, all together, have considerably restricted traditional intelligence collection activities and thus favored the use of cyber tools to carry out strategic espionage and reconnaissance (Check Point Software Technologies, 2020b). As a result, cyber intelligence has become the instrument of choice of many countries with the associated capabilities, particularly as the risk calculus is so favorable to the attackers – i.e. perceptions of a low risk of escalation but high potential reward.

Due to the urgencies wrought by the pandemic, previous grievances or strategic interests have become less salient and apparently receded into the background as media attention on the pandemic crowded-out many of these issues. Despite the lack of media attention, they have not disappeared, as proven by the various ongoing sophisticated cyber campaigns that show no immediate

nexus with the pandemic. This realization underpins several open-ended questions. The first being how and to what extent has the change in focus affected other types or ongoing cyber operations? Related to that, to what extent are some malicious actors able to continue such activities in light of the impending economic or budgetary pressure? Pertaining to the last one, one supposition is that these programs attempted to supplement dwindling state revenues through cybercrime.

1.3 Relative Continuity in Adversarial Behavior

As the last sections have shown, the coronavirus pandemic has brought unprecedented change to the physical and digital worlds. It has fostered some socio-technical changes and an acceleration of digitalization that will have lasting effects in the months – and years – to come; effects that will affect the cyber threat landscape as malicious actors exploit these new avenues.

Despite what could at first appear as fundamental changes in the cyber threat landscape and adversarial behavior, a number of its elements have remained relatively unchanged 5despite the crisis environment. This notably includes the type of active actors(see section 2.1), the type of malware and techniques deployed (see section 2.2.), and the overall volume of certain types of attacks (e.g. phishing and malspam). Accordingly, the threat landscape that has emerged during the pandemic is shaped by a number of pre-existing conditions.

The first similarity to threat assessments from before the pandemic to underline is that cyber threats are by nature inherently dynamic, fluid, and reactive. Indeed, threat actors tend to continuously innovate to find new ways to avoid detection, to attain their objectives, or to exploit some new avenues and opportunities. As a result, they adapt their social engineering schemes, cybercrime services, and malware to current events (e.g. to take advantage of elections to military clashes) to ensure their success. This has particularly been the case in time of crises, which often provide additional opportunities for exploits and catalyze malicious efforts beyond the baseline usually observed (see section 1.1). Themes, attacks, and business models come and go and, depending on the issue, are sometimes adapted and reused. This was also the case for many coronavirus-related cyberattacks, which were in many cases former Ebola-themed attacks with a simple word switch (Cimpanu, 2020b; Mouton and de Coning, 2020). Threat actors have also been fluid and adaptive throughout the different phases of the pandemic across the globe, exploiting, turn after turn, any attention-worthy events – e.g. lockdowns, transitions, reopenings, financial aid, unemployment, medical leave, etc. This opportunism and dynamism have not faltered, meaning threat actors will continue to leverage any newsworthy developments around the pandemic (e.g. new lockdown, second wave, etc.).

The second similarity is that the cyber threat actors active during this pandemic are essentially the same as before the crisis, although they slightly modified their operations and business model to best exploit the crisis (Europol, 2020c). For instance, most of the active APTs observed during this pandemic have been in operation since before the pandemic – some of which have been pursuing a variety of geostrategic goals unrelated to the pandemic (Europol, 2020c). There has been, however, a slight increase in the number of amateur cybercriminals (i.e. linked to opportunity and financial pressure), whose attacks mostly fall on the lower end of the spectrum and were accounted for in the early spikes in phishing attacks. Other established actors, meanwhile, largely pursue the same objectives, be it financial or strategic. And while it is true that medical espionage did take priority during these first months of the pandemic, it is primarily a new and time-bound facet of the ongoing greater strategic game between nations states.

The third similarity relates to the techniques, infrastructure and malware used by these same actors. Apart from some exceptions, such as the resurgence of *Zeus* and double-extortion ransomware, the techniques and malware that are deployed are largely the same as before the crisis, only repurposed from former campaigns (e.g. *Emotet*, *Agent Tesla*, *Trickbot*, *Lokibot*, and *Formbook* – see section 2.2.5) (Joyce, 2020; Microsoft Threat Protection Intelligence Team, 2020). Furthermore, some threat actors have continued to exploit old and new vulnerabilities before they were patched. As such, this lack of innovation can probably be linked to an inherent cost-benefit logic as long as existing tools retain – if not increase – their effectiveness in the current environment.

Lastly, despite the large increase in percentages of coronavirus-related attacks, such cyberattacks only comprised a small amount of the overall threat volume (Lefferts, 2020; Muncaster, 2020b; nixu, 2020). In April, Microsoft wrote that of the millions of emails it sees and scans daily, only 60,000 included COVID-19-related malicious attachments or malicious URLs, which amounts to less than two per cent[15] of the total malicious email (malspam) traffic. Instead of a spike in traffic, Microsoft said that cybercriminals have merely changed email templates and subject lines (lures), switching from regular invoice-themed lures to coronavirus-related topics (Cimpanu, 2020c; Lefferts,

[15] While these percentages need to be nuanced and put into perspective, they still illustrate a trend towards a low volume of COVID-19-related cyber threats compared to the level of threats generally.

2020). In addition, the Microsoft Threat Protection Intelligence Team later claimed that even the peak of coronavirus-related attacks in the first two weeks of March was "barely a blip in the total volume of threats we typically see in a month" (Microsoft Threat Protection Intelligence Team, 2020; Muncaster, 2020b).

Furthermore, the general level of phishing emails, spam emails, malicious URLs, and malicious email attachments has remained similar to previous periods. Taking Kaspersky's reporting for Q1 2020 for illustration, the largest share of spam was recorded in January (55.76 per cent) and the average percentage of spam in global mail traffic was 54.61 per cent, down 1.58 percentage points compared to Q4 2019 (Shcherbakova et al., 2020). For the same reporting period, Kaspersky's solution detected a total of 49 million malicious email attachments, which is almost identical to the figure for the last reporting period. Indeed, the absolute number of malicious attachments detected in Q1 2020 dropped by 314,000 compared to Q4 2019 (Shcherbakova et al., 2020).[16]

1.4 Takeaways for the Future

Looking at both, the novelty due to the pandemic and the overarching continuity of the cybersecurity threat landscape as such, there are a number of takeaways and considerations that seem to be relevant for the future, particularly as many countries brace themselves for a second wave of infections and a possible lockdown.

One first takeaway is that the volume and damage done by cybercrime have been steadily increasing over the past years and that the coronavirus pandemic will only reinforce this trend, as the economic pressure will further incentivize individuals' recourse to cybercrime as a means of income. These economic drivers will become more structural as the gains and knowledge acquired during this pandemic will encourage aspirant cybercriminals to continue.

In practice, while the observed surge in online scams, phishing, and BEC related to the coronavirus has already somewhat stabilized and rescinded, it will not disappear. The general levels of cybercrime observed will probably remain higher than before the crisis (Interpol, 2020a). Meanwhile, as long as the coronavirus remains an ongoing issue, one can expect cybercriminals to leverage the theme. As we move forward in this crisis, one topic, in particular, that may catalyze the attention of the public and private sector – and thus offers new opportunities to cyber threat actors – will be the issue of vaccine development and distribution as well as any information pertaining to new waves of infections and renewed lockdowns.

Thus, as the cyber threats continue to grow and adapt, the importance of cybersecurity awareness-raising, capacity building, and communication for all stakeholders needs to be underlined. Particular efforts should be made around authentication methods, such as the rigorous verification of credentials and deployment multifactor authentication. Indeed, one of the main increasing threats of this first half of 2020 has been identity-based attacks using brute force on enterprise accounts (e.g. for Zoom, VPNs, email accounts etc.). This critical first step would considerably harden the cybersecurity of many institutions and complicate many – now automated – exploits.

At the same time, responsible authorities (e.g. public and private CSIRTs) should especially capitalize on the attention the issue of cybersecurity has received in the last few months to promote and build upon the efforts, resources, and communication channels developed during this pandemic. These efforts should not be restricted to telework themes but broadened to the evolving threats posed by the digitization processes spurred by the pandemic. Initiatives such as the WHO's CYB4COVID resources compendium and the ECSO's Cyber Solidarity campaign are only two among a myriad of worthy examples that could serve as inspiration.

Another important lesson learned concerns threat intelligence. This pandemic has highlighted the importance of information exchange, cooperation, and coordination between all stakeholders. The urgency of the cybersecurity situation – notably for healthcare organizations – has led to a renewed engagement, be it in the form of round tables with third parties, contact points, common reporting, or dedicated networks, and initiatives. As we move forward, all of these advances need to be consolidated and built upon, especially as these dynamics not only fostered a better understanding and more comprehensive view of the evolving cyber threat landscape but also supported coordinated response and communication, which are central to better preparedness. These steps have facilitated the identification – and sometimes remediation – of redundancies and bureaucratic hurdles (e.g. intelligence classification rules for third parties such as critical infrastructure) that have undermined information sharing in the past. Most importantly, this engagement has also helped tighten the cybersecurity/CSIRT community at large and fostered trust and personal contacts, two crucial components in times of crisis.

However, a critical challenge for quality threat intelligence has been information overload. While public reporting by commercial cyber threat intelligence companies can be very useful – notably for advancing open-source intelligence (OSINT) analysis – without

[16] As a caveat, other types of attacks, such as ransomware or brute force attacks, or attacks against the cloud, have indeed become more prevalent during this period (see section 1.2.2 and 2.2.5).

appropriate contextualization it can create "intelligence noise" and biased/sensationalist reporting.

Another finding is that policymakers and cybersecurity professionals should not underestimate the accelerating impact the coronavirus has had on the digitalization of our economies and societies, and the threats and vulnerabilities that have emerged as a result. Among these, the normalization of teleworking and use of cloud-based services stands out. As countries continue to experience different types of lockdowns and a resurgence of coronavirus cases, we are experiencing a renewed increase of remote work. As such, the various risks and vulnerabilities described throughout this report will remain relevant – with new ones emerging. However, compared to the situation in the early months of 2020, companies and organizations should have had enough time – and if not, should start – to invest in infrastructure to support a sustainable and secure shift to telework. This includes, among others, investing time and money in corporate devices, identity and access control/management, awareness-raising programs for employees, contingency and internal reporting protocols/systems, and the recruitment of new talent. This also includes the shift toward more "new school",i.e. automated, cybersecurity technologies and practices, such as pattern recognition and predictive analytics against malware or automated detection of abnormal network resource allocation against DDoS attacks. This shift to automation would allow for a more efficient allocation of a limited cybersecurity workforce.

Furthermore, policymakers, product designers, and company leaders must also realize that a sustainable and secure shift toward telework is not possible without properly addressing cloud security – including some interlinked challenges such as 5G – and that of cloud-based applications/services. As mentioned in this report, widely popular cloud-based applications and services, such as Zoom or Microsoft Teams, have suffered from security vulnerabilities and the scrutiny of malicious actors due to their popularity. Furthermore, the rise in cloud-based applications and telework indicate a probable continuous increase in Internet traffic, with all that this entails in terms of criticality and vulnerability of ISPs, increasing intensity of DDoS attacks, and the general digital noise that make threat detection more complex.

Meanwhile, SMEs and small actors that had to digitize hastily to survive economically remain, for the most part, immature in terms of cybersecurity and thus run the risk of being targets in the near future. Indeed, threat actors who had concentrated their efforts on larger – more profitable – unsecured organizations and infrastructure during the peak of the crisis – e.g. hospitals – will probably shift their focus towards the low-hanging fruits that are these less well-resourced actors. As such, this calls for even more awareness and capacity buildings for these stakeholders. As they remain one of the hardest stakeholders to reach in terms of providing cost-effective cybersecurity, it seems essential to find new ways of getting to them, whether by tailored products, dedicated campaigns, events, or passive communication channels such as newsletters. In addition, the shift towards a cashless and digital economy also means that more carding fraud is to be expected, particularly as detection of fraud becomes harder due – in part – to the increase in financial transactions as well as the quantity of new entry points in the global transaction system.

The final consideration is that geopolitical competition and tensions are on the rise and will probably continue on this trajectory. This dynamic is particularly anchored in the efforts to find, and later distribute, a vaccine – which may include espionage on research, confiscation of essential supplies for the production of vaccines or the rerouting of actual vaccines, and disinformation about the effectiveness and safety of vaccines. As a result, policymakers should expect a constant – if not increasing – level of sophisticated cyber threats against critical infrastructure, especially organizations involved in vaccine research and production, as well as disinformation around the issue. This is even more true as, fueled by countries willing to pursue vaccines at significant cost and the general international calendar (e.g. US elections), the window of opportunity for de-escalation between great powers is narrowing – at least in the next few months.

Concerning healthcare, despite the absence of grave repercussion – apart from funds lost in ransom schemes and loss of strategic or economic advantage through espionage – the pandemic has highlighted the well-known cybersecurity deficiencies in the healthcare sector and provided a glimpse into how these cybersecurity risks could impact crisis responses. This wakeup call – or at least mobilization of political elites – should be leveraged not only to promote and invest in dedicated awareness-raising, updated systems, and capacity building (e.g. of the medical staff) but also rethink the general cybersecurity approaches for key critical infrastructure to build up their cyber-resilience. On top of the traditional top-down cybersecurity injunctions and support structures, the pandemic has offered us a glimpse of a promising form of bottom-up mobilization (e.g. the various cybersecurity community militias that helped defend the health sector) that should be built upon and further developed.

Concerning disinformation, the development of new and the improvement of existing technologies (e.g. AI-powered text generations or the proliferation of deepfake capabilities) coupled with the noxious international and national climates tend to indicate that large-scale disinformation is generally here to stay. This is also true about mis- and disinformation around the coronavirus. Spurred by the pre-existing domestic divisions and mistrust and leveraged to create new ones, coronavirus-themed disinformation will remain

prevalent, particularly as the subject will continue to permeate most public, political, economic, and private discussions.

2 Cyber Threat Landscape: Overview of Different Coronavirus-Related Cyber Threats

To better qualify and illustrate these developments and their implications, the following paragraphs provide a general snapshot analysis of the various cyber threats observed for the first half of 2020 – i.e. from January to the end of June 2020. The chosen focus and emphasis is on coronavirus/COVID-19-related cyberattacks and threats. To do so, the first subsection describes (2.1) the various active threat actors and their aims, such as cybercriminals and state sponsored threat actors. The second subsection (2.2) lays out a variety of the type of threats, from phishing and malware campaigns to BEC and DDoS. As a disclaimer, this subsection is based on traditional threat reporting categories. Finally, the last subsection (2.3) focuses on notable targets of these attacks and their geographical distribution.

2.1 Actors and Aims

Among the five types of threat actors generally recognized in threat intelligence reporting – namely cybercriminals, state-supported groups (or Advanced Persistent Threats (APTs)), script kiddies, insider threats, and hacktivists – cybercriminals and state sponsored actors have been the most active/visible in exploiting the ongoing health crisis. The others, while likely active, have seemingly posed less of a threat and are thus not covered in this report.

2.1.1 Cybercriminals

The first type of actor that has been considerably – if not the most – active during this pandemic are cybercriminals. In contrast to state-sponsored actors, their goal is predominantly financial. Only a small subset is engaged in sowing destruction, disruption, panic, or confusion. The outbreak has been leveraged by the whole spectrum of cybercriminals, from professional and well-established cybercrime groups to aspiring or opportunistic cybercriminals.

At the lower end of the spectrum, the coronavirus crisis has attracted a number of amateur or aspiring cybercriminals – sometimes referred to as script kiddies turned bad – some of which were criminals (e.g. drug dealers) that saw their criminal livelihood threatened by the lockdowns. Most actors of this group possess limited programming knowledge and skills. These seem to have acted due to a confluence of factors, which are, to a certain degree, also valid for more sophisticated actors (Europol, 2020c). Described in more detail in section 1, these are: the high demand for paired with scarcity of certain goods; an increase in available time due to a reduction in individual mobility or workload (e.g. due to layoffs); and an increase in malicious tools available on underground forums.

At the more advanced end of the spectrum, criminal actors have equally seized on uncertainty and fear related to the pandemic as an opportunity to trick users into unsafe behavior. Indeed, researchers and journalists have reported several campaigns by known cybercriminal organizations and groups. Anecdotally, this includes the Russian threat actor 505 (aka. TA505), which is known for their large campaigns, experimentation with a variety of malware delivery mechanisms, and distribution of ransomware, banking Trojans and RATs (Degrippo, 2020a; F & Scholten, 2020). In March, it was reported that they used coronavirus lures – including emails with the subject line “protect your friends” – to infect victims, primarily employees at US pharmaceutical and manufacturing companies, with an embedded *Get2Loader* and *SDBbot RAT* (F & Scholten, 2020). The same group has also been sending coronavirus-themed malspam to healthcare, manufacturing, and pharmaceutical organizations in the US. The emails have the subject "COVID-19 Everything you need to know" and contain a link to a ransomware downloader that can be used to further infect an accessing machine (Cyjax, 2020). A separate TA505 campaign, targeting healthcare providers, requests a bitcoin payment, ostensibly to help develop "Remedies On Corona-Virus” (Cyjax, 2020; Degrippo, 2020a).

Another malicious group, TA564, that regularly targets users in Canada by posing as shipping companies, such as CanadaPost and DHL, has attempted to deliver *Ursnif*, *DanaBot*, and *Nymaim* Trojans in the past (F & Scholten, 2020). Researchers at security firm Proofpoint have attributed an email campaign targeting “parents and guardians” while spoofing the Public Health Agency of Canada to deliver the *Ursnif* Trojan (F & Scholten, 2020).

The Russian-speaking threat actor TA542 (aka Mummy spider) has also been reported to use coronavirus-related themes in various email distribution campaigns. Malicious documents distributed by the actor have embedded macros that act as a downloader for *Emotet* malware (Malwarebytes Threat Intelligence, 2020).

Groups engaged in business email compromise have also been leveraging the crisis and deploying adapted coronavirus-oriented attacks (see section 1.3.4). Among the known active groups are *Silent Starling*, *Curious Orca* and *Ancient tortoise* (Gatlan, 2020).

The Nigerian cybercriminal organization *Scattered Canary* been behind the massive fraud against unemployment insurance programs in various US states, including Florida, Massachusetts, North Carolina, Oklahoma, Rhode Island, Washington, and Wyoming – with potential losses exceeding 100 million USD (Hassold, 2020; Krebs, 2020b). According to researchers

from the cybersecurity firm Agari, evidence has also been found that links *Scattered Canary* to previous attacks targeting CARES Act Economic Impact Payments, which were meant to provide relief in response to the coronavirus pandemic, as well as new scams targeting Hawaiian unemployment benefits (Hassold, 2020).

Organized ransomware gangs have also leveraged the current pandemic and continue to present a significant threat to businesses in all sectors, particularly to healthcare organizations and other critical infrastructure operators across the board – e.g. targeting government facilities, education institutions, and within the energy and food industry. Groups including *Maze, Doppelpaymer, Sodinikobi/REvil, Pwndlocker, Ako and Nefilim* have used coronavirus lures to infect a broad range of organizations, encrypting their systems after stealing sensitive information and then publicly leaking data if the ransom is not paid (Cyfirma, 2020). Victims have been diverse and include utility sector contractors, petroleum suppliers, retailers, or IT service providers (Cyfirma, 2020).

***

Overall, the general observation regarding cybercriminals echoes the conditions laid out in section 1.3, which note a lack of radical change in the cyber threat landscape and general continuity and combined with targeted adaptation. On the one hand, we observe a new wave of amateur cybercriminals fostered by the economic and socio-technical context – indications for which can be identified in the aforementioned volume of relatively unsophisticated attacks and the increase in the sales of grayware services/tools. On the other hand, the majority of professional cybercriminal threat actors observed remain – as could be expected – the same groups as before the pandemic using known or repurposed tools. Among these, some threat actors that were previously inactive have seemingly resumed their activities to exploit the situation. However, while the coronavirus crisis has undeniably been a boon for many cybercriminals, it is worth recalling that many have also continued their often well-established activities and schemes using non-coronavirus related lures.

One other noteworthy observation pertaining to cybercriminals' adversarial behavior has been the display of ethical and moral stances against the exploitation of the fear, death, and misery resulting from the coronavirus pandemic for financial gain. According to a report by the threat intelligence firm Digital Shadows, in the early months of the pandemic, discussions around COVID-19 had been very heated and attracted attention on the dark web – as much as on the clear web. While many discussions expectedly revolved around the best and different ways to exploit the then-looming coronavirus crisis, other atypical discussion threads had also been reported (CyberPeace Institute, 2020; Guirakhoo, 2020a; Photon Research team, 2020). These have notably focused on the ethicality of exploiting the crisis for financial gain, with many users discouraging others from promoting the exploitation of the pandemic. They also focused on providing health advice, up-to-date information on the infection trends and expressions of solidarity with those affected, particularly in Italy.

These seemingly humane and benign discussions correspond with vows of major ransomware groups, such as *Maze, DoppelPaymer, Ryuk, Sodinokibi/Revil, PwndLocker* or *Ako*, to not attack the healthcare sector(Abrams, 2020a). Anecdotally, this pledge took place after Lawrence Abrams – the creator of journal BleepingComputer – reached out to these cybercrime groups. Following these declarations, reports have confirmed preliminary signs of good faith, such as steps taken by the groups behind the *Maze* and *DoppelPaymer* ransomware in offering ransomware recovery services (i.e. decryption) to affected medical facilities free of charge or at a discounted rate (Winder, 2020). The *Maze* group has also removed more than 2300 highly sensitive medical files from former patients of Hammersmith Medicines Research (HMR) from its website (Intsights, 2020).

These unusual promises have nonetheless been problematic for several reasons. First, despite them, the attacks against critical medical facilities seem to have continued. For instance, in April, reports have shown that the *Ryuk* ransomware group had persisted in its efforts against the healthcare sector and targeted at least ten healthcare providers, including a healthcare network of nine hospitals. One of the hospitals targeted by the *Ryuk* ransomware was in a US state profoundly affected by the coronavirus pandemic (Hope, 2020b). Furthermore, by releasing patient data these groups also contributed to putting the concerned individuals in harms' way even more.

Second, while such promises – if ever respected – might have been made by some of the major actors–a considerable number of other malicious actors remained active without any measure of self-restraint. These actors recognized the opportunity and readily filled the gap. This is notably illustrated by the number of attacks against the medical sector described later in section 2.3. In addition, these promises only concerned the health sector. A number of other critical sectors and institutions that helped respond to the pandemic (e.g. the food and energy industries, education institutions, and others) continued to be targets of such attacks.

Third, this display of what might appear as "honor among thieves" remains highly dubious. While cybercriminals might even be personally affected by the pandemic (including through family or friends) these declarations, at least from major groups, seem to have been more motivated by self-preservation than by empathy or ethics. Indeed, due to the amount of media coverage of these attacks and the public outcry that they generated, there might have been a concrete fear that they would attract a forceful response from law enforcement agencies and the cybersecurity community

at large. This seems to be particularly true as there has been a considerable amount of bottom-up mobilization by the community – in the form of cybersecurity militias (e.g. the COVID CTI League) – to help fight attacks against the health sector (Scammell, 2020).

2.1.2 States and State-Sponsored Actors

Despite the widespread social, political, and professional disruption, state and state-sponsored actors have been active in cyberspace during this pandemic. This comes without surprise as, from the 2015 Paris attacks to the Ebola pandemic, state-sponsored groups have often leveraged and exploited current tragic world event to advance their financial or strategic aims (Cimpanu, 2020b).

The aims of these groups vary and are often ambiguous. Some state-sponsored groups have sought to exert influence, whether by shaping or altering narratives in the context of government responses to the coronavirus outbreak. One blatant example includes the attempts by both the US and China to steer the narrative around the origin, subsequent spread and responsibility for the rapid proliferation of the coronavirus in the early months of the pandemic. To pursue this, they used a variety of cyber-enabled influence operations (CIO) and techniques, such as a mix of white (i.e. official source), gray (i.e. unknown source) and black (i.e. usurped source) propaganda across a variety of platforms[17] (DiResta, et al., 2020).

Another aim has been disruption (e.g. of the response against the coronavirus), whether by fostering distrust or sowing confusion between the population and the government. This was notably the case in early February in the US, where coordinated efforts to spread disinformation (e.g. conspiracy theories) and to alarm about the pandemic were observed (Glenza, 2020). According to the US State Department, thousands of Russian online accounts – previously identified as involved in disseminating Russian-backed messages related to major events such as the war in Syria, the Yellow Vest protests in France and Chile's mass demonstrations – were behind the spread of some of these messages (Glenza, 2020).

Disruptive cyberattacks (e.g. through ransomware) were also observed against critical infrastructure (CI). The pandemic has heightened the risk profile of critical (information) infrastructure, due to the potential catastrophic and life-threatening after-effects. One notable case was observed in mid-April when two Czech hospitals were attacked by – according to an anonymous Czech official – a "serious and advanced adversary" (Reuters, 2020a, 2020b; Wiggen, 2020). Specialists meanwhile have also observed some degree of espionage. The general lack of information around many aspects of the current crisis has led a number of states to resort to cyberespionage to gain vital strategic information, including on the spread of the coronavirus, different national policies for containing the virus, and potential drugs as well as vaccines (Wiggen, 2020). A number of these cases against western medical institutions and governments have been denounced and attributed to various threat actors from China and Russia (National Cyber Security Centre, 2020a, 2020b).

While the full extent to which states have engaged in such activities can never be totally uncovered, Google, in April, detected over a dozen state-sponsored hacking groups using the coronavirus to craft phishing emails and attempt to distribute malware (Huntley, 2020). Microsoft observed 16 different nation-state actors either targeting customers involved in the global COVID-19 response efforts or using the crisis in themed lures to expand their credential theft and malware delivery tactics (Burt, 2020). The following paragraphs describe the discovered operations, ordering them by their "assumed" affiliated nations. As a renewed caveat, these observations are by and large based on publicly available threat reports from western firms and thus may contain biases as to the actors studied.

China

Chinese threat actors (e.g. *Emissary Panda*) have been very proactive during this pandemic. Indeed, in early March – which corresponds to the time when the Chinese infection rate was slowing down – China was one of the main points of origin for spear-phishing and malware campaigns leveraging coronavirus lures (Cimpanu, 2020b). Some of these campaigns specifically revolved around US COVID-19 research, as declared by the US Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) (FBI and CISA, 2020; Wiggen, 2020). It is possible that other nations were targeted by similar cyberespionage endeavors.

In addition, the two Chinese APTs *Mustang Panda* and *Vicious Panda* were discovered to have targeted various individuals and elements of the public sector in Vietnam, Mongolia, Taiwan, and the Philippines with phishing emails containing spyware (in this case, targets received messages with a compressed file archive in the attachment that installed a Trojan) (Cimpanu, 2020b; Intsights, 2020). These emails were purporting to carry coronavirus-related messages from authoritative and official sources, such as the Vietnamese prime minister or the Mongolian ministry of

[17] For an in-depth discussion of Chinese influence efforts during the pandemic please see the forthcoming CSS Cyberdefense Report "Active Control and Covert Enablers" by Jakob Bund.

foreign affairs. The aim was to take screenshots, exfiltrate, delete and edit files, and to remotely execute processes (including through the use of penetration testing tools like *Cobalt Strike* or the *PlugX* remote access Trojan) (Cimpanu, 2020b; Intsights, 2020).

Russia

In addition to the aforementioned coronavirus-related disinformation campaign targeting the US that has been linked to Russian accounts, the cybersecurity community detected one other major Russian campaign perpetrated by the *Hades* group, which has ties to *APT28* (aka *Fancy Bear*) (Intsights, 2020). The US and the UK have previously identified *APT28* as operated by the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU) (National Cyber Security Centre, 2018; US District Court Western District of Pennsylvania, 2018). Specifically, the group in mid-February engaged in a multifaceted campaign – dubbed "Tricky Mouse" – against Ukraine (Malwarebytes Threat Intelligence, 2020).

In its first phase, the campaign included a large-scale phishing campaign imitating the Ukrainian Center for Public Health and containing a lure with fake documentation about COVID-19. Similarly to the aforementioned Chinese cyberattack, the documentation included a hidden C# backdoor Trojan that gave remote control of the device (Intsights, 2020). The second phase was a disinformation campaign conducted through social media. It mainly focused on disseminating fake reports on the increasing number of COVID-19 infections in Ukraine, coinciding with the arrival of a flight of evacuees from China and COVID-19 patients from eastern Ukraine (Intsights, 2020). While direct causality is hard to establish, the operation seems to have been somewhat successful as protest did emerge in several parts of the country with reports that protesters blocked the access to some hospitals (Cimpanu, 2020b).

Russia has also engaged in espionage targeting vaccine research and espionage on intellectual property across the western world, notably through *APT 29* (aka *Cozy Bear*), which was found – as publicly reported by the UK's NCSC, the Canadian Communication Security Establishment (CSE), and the US's National Security Agency (NSA) – to target various organizations involved in COVID-19 vaccine development in Canada, the United States and the United Kingdom (National Cyber Security Centre et al., 2020). According to an assessment by the UK NCSC and malware samples disclosed by US Cyber Command, *APT29* has been using custom malware in these operations – i.e. WellMess and WellMail – which had not been previously publicly associated with the group.

Russian threat actors have also continued their previous campaigns but modified their lures to exploit COVID-19. One of these was operated by the APT *Gamaredon* (aka *Primitive Bear*), which apparently intensified its efforts to compromise Ukrainian defense and intelligence targets. The attacks include both cyberespionage and attempted sabotage of physical assets in mid-February (Council on Foreign Relations, n.d.; Malwarebytes Threat Intelligence, 2020).

Pakistan

Pakistan's *APT36* (aka *Transparent Tribe, ProjectM, Mythic Leopard,* and *TEMP.Lapis*) also sought to take advantage of the opportunity presented by the crisis to further its espionage activities – notably against India's defense establishment, embassies, and other government agencies (Threat intelligence team, 2020). Specifically, threat intelligence researchers have found that the group was spreading a malicious document spoofed to look like it came from Indian government websites. Once opened, the document enabled macros, which executed the Crimson RAT payload, which is used for a wide range of cyberespionage activities, including stealing credentials; listing running processes, drives, and directories on the victim's machine; retrieving files from its command and control (C&C) server; using custom TCP protocol for its C&C communications; collecting information about antivirus software; and capturing screenshots (Cimpanu, 2020b; Threat intelligence team, 2020).

India

In early February, the reportedly Indian APT *Patchwork* (aka *Dropping Elephant, Candlefish, Chinastrats, APT-C-09, Quilted Tiger*) was identified to be sending phishing emails with a COVID-19 theme, using malicious Excel documents to target Chinese organizations in Wuhan, triggering a Chinese patriotic hacktivist retaliation (iDefense, 2020; Malwarebytes Threat Intelligence, 2020). It also reportedly targeted Pakistan with a phishing attack using information regarding an alleged local Pakistani Army deployment to help combat COVID-19 (iDefense, 2020).

Iran

Iran, which has acutely suffered from the pandemic, recording the highest death toll in the Middle East, seems to have been desperate for intelligence and information related to the spread and treatment of the virus. While no definite proof has been made public to date, an Iranian backed threat actor has allegedly been behind a wave of phishing messages in March that were directed against the WHO in an attempt to access its digital systems (Bing et al., 2020). According to some reporting, this attack would be consistent with methods used by *APT35* (aka *Charming kitten, Phsophorus, Ajax security, Newsbeef*) (Satter et al., 2020). Later in April, the same APT group seemingly launched a number of

phishing attacks against the pharmaceutical company Gilead Sciences, which has been working on the development and distribution of treatments for COVID-19 (Stubbs and Bing, 2020).

Syria

A group using similar IPs as the *Syrian Electronic Army*, which operates out of multiple cells both within Syria and in neighboring countries, reportedly used COVID-19 as lure to get users to install mobile applications targeting Arabic-language users; these malicious apps had names such as "Covid19," "Telegram Covid_19," "Android Telegram" and "Threema Arabic," among others (Paganini, 2020).

North Korea

In late February, South Korean officials received phishing emails with malicious documents attached that claimed to provide information on how the South Korean government planned to deal with the coronavirus crisis (Intsights, 2020). The emails contained malicious documents weaponized with a spyware called *SpyLoop*, which continuously collects and sends device/user information (Malwarebytes Threat Intelligence, 2020). Although not as sophisticated as the Russian campaign, the phishing campaign aimed at South Korea delivered *BabyShark*, a malware strain previously utilized by a North Korean hacker group known as *Kimsuky* (aka *Velvet Chollima*) (Intsights, 2020; Malwarebytes Threat Intelligence, 2020).

Another North Korean APT active during the first half of 2020 has been *APT37* (aka *Konni*). In mid-March, the group was recorded as sending spear-phishing messages, notably to South Korean targets, containing COVID-19 warnings, ironically advising readers to watch out for spikes in North Korean cybercrime related to the spread of the virus (Malwarebytes Threat Intelligence, 2020).

The *Lazarus Group* has also been using coronavirus lures to target different cryptocurrency businesses to steal cryptocurrency for financial gain (GreAT, 2020a). The same group has also targeted six countries – namely Singapore, Japan, Korea, India, the US, and the UK – which had announced significant financial support for businesses reeling from coronavirus restrictions. The hacking campaign involved phishing emails that looked like they came from various authorities in charge of COVID-19 support initiatives dispensing government assistance. The over five million phishing emails were designed to drive potential applicants to fake websites that farmed credential and other personal information (Cyfirma, 2020).

South Korea

According to contested reporting by the Chinese cybersecurity firm Qihoo 360, *DarkHotel*, which has possible ties to South Korea and has previously been active in East Asia, has launched an apparent espionage campaign against Chinese government institutions and agencies. The campaign has sought to exploit over 200 VPN network servers – notably using a zero-day exploit to gain control over Sangfor VPN servers (Stone, 2020a). The report by Qihoo 360 said that 174 of these servers were located on networks of government agencies in Shanghai and Beijing as well as the networks of various Chinese diplomatic missions (e.g. in Italy, UK, Pakistan, India, and Israel) (Cimpanu, 2020d). In addition, the same group apparently also conducted operations against the WHO, for which it set up a fake website spoofing the WHO's internal email domain to steal credentials (Bing et al., 2020).

Vietnam

Starting in February, *APT32* (aka *Ocean lotus, Sea Lotus*), which regularly targets the private and public sector in Southeast Asia, has been observed using malicious macro-embedded documents with coronavirus themes to target Chinese targets (iDefense, 2020; Malwarebytes Threat Intelligence, 2020). In this *METALJACK* attack, the malicious document dropped the *Denis* Trojan, a malware family that has been developed by this group (Malwarebytes Threat Intelligence, 2020).

***

As for cybercriminals, the main observation regarding state-sponsored threat actors is one of relative continuity, at least in terms of the active actors themselves. Most of the state-sponsored activities detected can be linked to known groups – this ties in with the observation that no new major actors appear to have been discovered during that period. This finding is owed in part to fact that, as is commonly the case, most newly recorded malicious campaigns are not immediately attributed to specific actors. There are of course anecdotal exceptions to this trend, such as the possibly new threat actor of unknown origin claiming to be threats groups *APT28* and the *Armada collective* to conduct extortion by DDoS in the US (NJCCIC, 2020).

As has been the case before the pandemic, the level of sophistication of the attacks by different threat actor groups seems to vary across the board. However, it is clear that APT groups, similarly to cybercriminals, have opportunistically exploited the COVID-19 pandemic as a theme – this, however, does not represent a shift in terms of their techniques, tools, and processes. Furthermore, it must be underlined that it has been recorded – albeit not explored in detail here as it is outside of the scope of this report –, that most APT actors seem to have continued their non-COVID-19-

related cyber operations. For instance, in April, Iranian-backed threat actors allegedly attempted to hack into Israel's water infrastructure. However, the extent to which state-sponsored threat actors' operations have generally been disrupted by the pandemic's socio-technical and operational changes remains unknown – and will probably stay so in the following months or years.

Finally, as previously underlined in this report, geopolitics remain – without surprise – an important motive for APT actors. This is particularly visible in terms of their choice of targets, most of which were aligned with their regional and strategic interests. In the context of the pandemic, this included national and international health and research institutions but also the public sector and armed forces all around the world. Most notably, Southeast Asia was a very active region for APT activities during the first half of 2020, with Chinese-speaking groups launching campaigns both within its neighborhood (e.g. across Central Asia) and against adversaries (e.g. US or Europe). China was also targeted early on by other regional actors, such as Indian, Vietnamese, and South Korean APT groups.

Meanwhile, state-sponsored cyber actors locked into well-established rivalries or conflicts have also leveraged the pandemic to their ends. As shown earlier, this includes Russian threat actors in Ukraine, Pakistani and Indian actors against each other, or Syrian actors in the neighboring countries.

2.2 Types of Cyber Threats: Tactics, Tools, and Procedures

Various threat actors have leveraged a great variety of tools and tactics to achieve their aims (see *Table 1* for an overview). The following section describes, exemplifies, and seeks to quantify the most frequently encountered forms of malicious cyber activity related to the coronavirus pandemic. As a note, the first two address specific threats to the teleworking infrastructure and mobile devices, both of which have been particularly affected by the pandemic, while the last six subsections address relatively general and prolific threats, some of which sometimes overlap as part of the same attack chain.

Table 1: Overview of COVID-19-related cyber threats by actor type (author's design, based on sources listed in this report)

X = Confirmed ? = Unconfirmed	Criminals	APTs
Credential Stuffing	X	X
RDP Brute Force	X	?
Vulnerability Exploits (e.g. VPNs)	X	X
Zoom Bombing	?	?
Fake COVID-19 Apps	X	?
Mobile Malware	X	?
Scams & Fraud	X	?
Extortion	X	
(Spear-)Phishing	X	X
Domain & URL Spoofing	X	X
Ransomware	X	?
Data Wiper	X	
Crypto-miner	X	X
Trojan – Spyware	X	X
BEC	X	
Malspam	X	X
DDoS	X	?

2.2.1 Teleworking Infrastructure Threats: Credential Stuffing, RPS Brute Force, and Vulnerable Teleworking Applications

A particularly important coronavirus-related cyber threat trend has been the rise of cyberattacks against teleworking infrastructure and applications. With the mass movement toward telework malicious actors have increasingly exploited a variety of cloud-based teleworking tools and software, such as conferencing applications and VPNs (Cybersecurity & Infrastructure Security Agency and National Cyber Security Centre, 2020; McAfee, 2020a).

With regard to the malicious use of cloud-based conference applications, Skype led the pack in April with at least 120,000 suspicious files using its name for both malware and adware (Whitney, 2020). Regarding other applications, a study from cybersecurity firm Kaspersky found that out of 1300 suspicious files they discovered and analyzed, 42 per cent were disguised as Zoom, 22 per cent as WebEx, 13 per cent as GoToMeeting, 11 per cent as Flock, and 11 per cent as Slack (Whitney, 2020). Zoom has been most targeted, seemingly due to its rising popularity.

Credential stuffing attacks [18] have been the most common type of attacks against these services, with threat actors trying to compromise accounts to sell them on hacking forums. Cracking communities such as *Cracked*, *Nulled* and *Raid Forums* have all released configurations for common credential stuffing tools,

[18] I.e. an automated brute force attack based on leaked credentials.

such as *Open Bullet* (Cyfirma, 2020). These configurations are offered for free and allow anyone with the software to begin stealing Zoom accounts. In one notable instance, a database containing over 2300 compromised Zoom credentials was leaked on the darknet. Victims included banks, consultancy companies, educational facilities, healthcare providers, and software vendors (Cyfirma, 2020; O'Donnell, 2020).

In addition, threat actors have created thousands of new domains containing the word "Zoom". As many businesses and educational institutions shifted to online platforms, many malicious actors have registered fake Zoom domains for their phishing attacks (Check Point Software Technologies, 2020c; Cybersecurity & Infrastructure Security Agency and National Cyber Security Centre, 2020). As of mid-May, the firm Check Point Software Technologies had recorded over 6500 new Zoom domains, 1.5 per cent of which were identified as malicious and 13 per cent as suspicious (Check Point Software Technologies, 2020d).

Regarding Zoom specifically, one of the most high-profile attacks/nuisances has been "Zoom bombing". This practice involves pranksters uninvitedly joining unsecured Zoom calls, usually to display offensive or illegal content. There have been several high-profile incidents. On 10 April, for instance, a US House Oversight Committee meeting discussing women's rights in Afghanistan was disrupted at least three times. This practice was greatly helped by the development of forums (e.g. "Zoom leaks") and tools (e.g. zWarDial) that discover and display unsecured Zoom meetings (Cyfirma, 2020).

On top of that, accidental exposure of recorded Zoom meetings has also been a concern. In April for instance, thousands of recorded Zoom meetings – e.g. business discussion, therapy sessions, sexual content from private calls – were made public, apparently by mistake. At least 15,000 exposed videos were discovered by a security researcher following a scan of unsecured cloud storage (Harwell, 2020). The problem lied in the file-naming system used by Zoom, which, combined with a user accidentally uploading the private file to the internet from their computer, made them easily discoverable (Harwell, 2020).

In addition, reports have also indicated that there has been a spike of interest in vulnerabilities of popular online platforms, notably for industrial espionage. Data from the threat intelligence firm Insights shows that malicious actors discussed and attempted to exploit different online platform vulnerabilities (Intsights, 2020). The main targets have been Zoom, Webex, and Microsoft Teams (Franceschi-Bicchierai, 2020a). Reports in April indicated that two critical zero-days vulnerabilities – which allowed to hack and spy on calls – for the Windows and MacOS Zoom applications, were for sale on the web (Franceschi-Bicchierai, 2020b). Also in April, Zoom was hacked and 500,000 stolen Zoom passwords were offered for sale on the darkweb.

Regarding VPNs, some threat actors (e.g. *Darkhotel)* have exploited VPN network servers for cyberespionage. Meanwhile, others have targeted VPNs as part of their DDoS attacks (see section 2.2.8). More generally, CISA in the US and the NCSC in the UK have observed actors scanning for publicly known vulnerabilities in Citrix. One vulnerability – i.e.CVE-2019-19781 – and its exploitation have been widely reported since early January 2020. Other examples include vulnerabilities affecting VPN products from Pulse Secure, Fortinet, or Palo Alto (Cybersecurity & Infrastructure Security Agency and National Cyber Security Centre, 2020).

2.2.2 Mobile Threats: Fake Apps, Mobile Malware, and Vulnerable Contact Tracing Apps

As mentioned in section 1.1, due to the increasing reliance and immature cybersecurity, mobile phones and connected networks and devices have increasingly become the target of threat actors, notably during the pandemic. The threats were varied and mostly took the form of smishing (i.e. phishing through SMS), fake or malicious apps, mobile ransomware and Trojans as well as attacks against official contact tracing apps.

During this pandemic – smishing , in particular, has been a growing threat to individuals and companies alike. As for email-based phishing, many of these attacks have leveraged COVID-19 themes. In South Korea, for instance, by mid-February, over 10,000 SMS had been sent to South Koreans pretending to come from companies providing free protective material (Mu-Hyun, 2020). During Q1 in the US, companies apparently recorded a 37 per cent increase in smishing (Schless, 2020). These attempts followed a variety of purposes, from malware dissemination to credential stealing.

According to the antivirus company Bitdefender, a huge spike in applications containing "COVID" or "corona" in their name, packaging, or file was registered in March. Researchers found that, in early March, Google Play listed over 2100 apps in Europe that used such keywords, compared to 500 in the US and around 1000 in Asia (Asoltanei et al., 2020). These apps varied from common medical information apps to newly developed or repurposed apps about the spread of the virus. Anecdotally, many non-coronavirus-related apps, such as games (e.g. Bubble Shooter Merge), have abused Google Play's ranking algorithm by adding coronavirus to their name to gain in visibility.

Some of the different apps – some of which were actually found on third-party marketplaces – had been repacked to include aggressive adware while others had been bundled with SMS-sending malware, ransomware or banking Trojans such as *Joker*, *Cerberus*, *GINP* and *Eventbot* (Asoltanei et al., 2020; Moran, 2020). For instance, the creators of a new modification of the *Ginp* banking Trojan renamed their malware "Coronavirus Finder" and then began offering it for 0.75 EUR disguised

as an app supposedly capable of detecting people nearby infected with the coronavirus (Chebyshev et al., 2020).

In addition, and for the first time, the *Anubis* banking Trojan was spotted as part of an Android coronavirus malware campaign. The application imitates a coronavirus information site and, on installation, asks for excessive access and permissions (Asoltanei et al., 2020). Initially, *Anubis* targeted countries ranging from the US and India to France, Italy, Germany, Australia, and Poland. This Android version, however, seems to have targeted Turkey, by impersonating the legitimate website to which it redirects users (Asoltanei et al., 2020).

In another case, an Android app which offered face masks and safety kits to worried individuals, delivered an SMS Trojan, which collects the contact list of the victim's phone directory and sends automatic SMS to discovered contacts to spread itself (Khan et al., 2020). In some iterations it also downloaded a mobile ransomware (Desai, 2020).

One particular well-reported ransomware case has been that of the new *CovidLock* malware, which circulated through the malicious Android app "COVID19 Tracker". After download, the ransomware locks the victim's phone, who is then given 48 hours to pay 100 USD in bitcoin to recover access. Similarly to other ransomware, threats include the deletion of the phone data and leakage of account information on social media (Khan et al., 2020; Sahel & Anderson, 2020).

As the pandemic progressed, malicious actors have adapted their targeting and methods. After leveraging the initial need for information with some fake tracking maps, some actors have turned their attention to governmental contact tracing apps. Indeed, with different governments around the world developing, releasing, and promoting their app, malicious actors have jumped on the occasion to exploit both these apps and the public campaigns for their adoption.

For instance, while the UK's National Health Service (NHS) app was still in the test phase, some unknown actor deployed and released a closely-resembling fake of the official app, which was in truth a banking Trojan (Smithers, 2020). The campaign attached to it also included an SMS phishing scam intended to make people believe they had been in contact with someone who had been tested positive for COVID-19 (Stone, 2020b). Another conspicuous discovered campaign has targeted Android users with a new ransomware called *CryCryptor*. It was distributed via two spoofed websites under the guise of an official COVID-19 tracing app provided by Health Canada (Stefanko, 2020).

More broadly, one report by researchers at the cybersecurity firm Anomali have found that at least twelve additional applications posing as coronavirus contact tracing apps – but not available on the Google Play app store – were designed to steal personal and financial information from unwitting Android users with various malware such as *Spynote*, *Anubis* or other Trojans and adware (Anomali Threat Research Team, 2020; Stone, 2020b). Targeted countries included India, Italy, Singapore, Iran, Russia, and Brazil (Anomali Threat Research Team, 2020).

With respect to the official contact tracing apps, there have been no reports of any being the subject of hacks or cyberespionage. This does not mean that none were compromised, especially as many of these apps have been developed in a hurry and have shown some vulnerabilities. In a recent study of 17 government-sponsored apps, the mobile application security firm Guardsquare found that less than a third had an encryption capability that protects sensitive information in the source code, and less than half had the ability to detect unauthorized requests that seek access to restricted data on the phone (Goodes, 2020; Starks, 2020).

The most striking case has been that of Qatar, where the mandatory contact tracing app – EHTERAZ – suffered from a vulnerability that would have allowed hackers to obtain the national ID numbers and health status of over a million individuals (Amnesty International, 2020; Starks, 2020). Another example is India's app – Arrogyasetu – where a researcher discovered a security gap that allowed him to determine who was sick in individual homes (Starks, 2020). Meanwhile, researchers have also uncovered seven security flaws in the UK's pilot app NHSX – some of which have since been addressed (Culnane and Teague, 2020). One of the Netherland's pilot apps – Covid19 Alert! – also suffered a leak exposing 200 names, emails, and encrypted passwords (Muncaster, 2020c).

2.2.3 Scams, Frauds, and Extortion

One of the main trends observed in the first half of 2020 has been the surge in coronavirus-related product frauds, scam templates and hoaxes on the clear-, deep- and darkweb markets. Scammers have been very creative and developed a great variety of scams, many of which exploited specific regional or national characteristics (e.g. tailored to legal requirements, local language, or new policies) alongside the general climate of fear, uncertainty, and stress described earlier.

The most common types of scams were around medical material, such as test kits, masks or fake treatments and drugs (Arsene, 2020). Indeed, during this pandemic, shadow pharmacies that promote a variety of drugs (e.g. for male erectile dysfunction) via spam or hacked websites have experienced a large increase in demand for treatment usually used to fight lupus, malaria and arthritis thanks largely to unfounded suggestions that these therapies can help combat coronavirus infections (Krebs, 2020c).

In March and April, hydroxychloroquine, for example, rivaled the usual primary products of such shadow pharmacies — generic Viagra and Cialis. The pseudo-treatment accounted for as much as 25 to 30 per cent of all sales in April (Krebs, 2020a). This sudden interest was particularly reinforced when various influential and public figures, including President Trump and Elon Musk in the US or Dr. Raoult[19] in France, started to suggested without sufficient scientific basis that it was an effective treatment for COVID-19 (Krebs, 2020a).

More sophisticated scams, targeting governmental procurement structures have also been conducted. One notable and sophisticated example includes a group of fraudsters that succeeded in getting the authorities in Germany's most populous region, North Rhine-Westphalia, to part with 2.6 million EUR. The money was a down-payment for ten million masks. More than 50 vehicles were lined up to import the fake masks from the Netherlands before the ruse was discovered. It involved a website registered in Spain, an intermediary in Ireland, and a firm in the Netherlands with a website that turned out to have been cloned by the scammers. With the help of financial institutions in three countries, investigators managed to block the payments, including 500,000 EUR on the way to Nigeria (The Economist, 2020).

In addition to the rise of coronavirus goods-based scams, researchers and agencies (e.g. the Internet Crime Complaint Center) have registered an increase in reports of online extortion scams (FBI, 2020a). These used scare tactics in an attempt to manipulate the users into paying bitcoin (on average the equivalent of 2000 to 4000 USD). Specifically, these scams leveraged prevalent paranoia and fear by threatening to infect the target's family with the coronavirus (Trend Micro, 2020a).

Another widely prevalent scam has used fake donation requests, which claimed to be relief or health organizations and asked for donations in bitcoin. One such example includes that of a group called COVID19Fund.

A last type of scams includes fraudulent shipping and insurance fees being charged by criminal actors. Opportunistic actors have citied false COVID-19-related updates to shipping laws, regulations, and requirements as justification for charging made-up fees. Examples have included fraudulent demands for COVID-19 insurance fees after a purchase for the delivery of live pets or a fake "refundable" shipping insurance fees (FBI, 2020b; Walter, 2020).

Indicator of Scale and Costs

According to security company Proofpoint, four out of five scam emails in March used coronavirus themes in some way (Ranger, 2020). Quantitatively speaking, in March alone, reports indicated a 400 per cent increase in coronavirus-related fraud, at least in the UK (Action Fraud, 2020a). For the same period, this amounted to over 500,000 messages, 300,000 malicious URLs, 200,000 malicious attachments with coronavirus themes across more than 130 campaigns (Ranger, 2020). By the end of April, the UK's NCSC had taken down 2000 campaigns and 471 fake online shops in the UK alone (Action Fraud, 2020b).

This rise in scams seems to be a general, opportunistically driven trend extending to other European countries – to various degrees. For instance, in Switzerland, the academically led website "coronafraud.ch" registered at least 160 cases of medical equipment scams in April (Soguel, 2020). This contrasts with the overall 2938 registered scam incidents registered by MELANI, the great majority being subscription scams (270), fake sextortion (578), and domain scams (63) (MELANI, 2020). The Swiss domain managing foundation SWITCH, however, did not necessarily assume that the number of fake webshops has increased during the lockdown period as most malicious domains using .ch or .li had been identified earlier (Städeli, 2020).

The financial loss associated with these scams has been considerable. In March, the UK's National Fraud Intelligence Bureau reported over 21 cases of such coronavirus-related fraud schemes, which, at the time, resulted in losses of over 800,000 GBP in the UK alone (Guirakhoo, 2020b). By the end of May, 4.6 GBP million had been lost to coronavirus-related scams with around 11,206 victims of phishing campaigns (Brunt, 2020). For comparison, in the UK, the cost of purchase scams in 2019 amounted to 59 million GBP (UK Finance, 2020). In the US the Federal Trade Commission claimed that at least 13 million USD had been lost to COVID-19-related scams in the first four months of 2020, with a median loss of 570 USD per scam (Cyfirma, 2020). The amount later soared to 145 million USD in September (PYMNTS, 2020). For context, the overall cost of scams for 2019 in the US stood at 1.9 billion USD (FTC, 2020).

2.2.4 Phishing and Social Engineering Schemes

Even before the pandemic, social engineering, by way of (spear-)phishing and spoofing (e.g. of domains, email addresses, and websites), was a very widespread technique, especially in the early phases of the attack chain. It is often only the preliminary step for an attacker to gain access, whether by stealing credentials or deploying malware (see section 2.2.5).

In the first six months of 2020, attackers have seized the opportunity to exploit the general global anxiety, uncertainty, and false information surrounding

[19] Based on his non-randomized research, the head of the Institut Hospitalo Universitaire Méditeranée – Dr. Raoult – declared as early as February 2020 that hydroxychloroquine was an efficient treatment against the coronavirus.

the pandemic. As a result, phishing emails have accounted for the majority of coronavirus-related malicious cyber activity (CyberPeace Institute, 2020; Interpol, 2020b).

In terms of format and delivery method, many variations of coronavirus-related phishing have been detected. As mentioned earlier, most were pushed through emails, but other vectors included SMS or social media (e.g. through Facebook Messenger). Two examples include a WhatsApp phishing campaign related to a fake relief fund. Another case used SMS delivery to steal credit card information and add an additional fee (Ducklin, 2020; Trend Micro, 2020a).

Lures have been varied, creative, dynamic, and responsive to new events (e.g. the setting up of relief funds). In addition, reports have shown that phishing attempts would often adjust language, content, and the imitated source on the basis of their targeted region and audience.

The targets of impersonation and spoofing have been as varied as the lures but can be divided into two categories. The first being well-established and trusted international and governmental institutions in various fields. Health-related institutions, such the WHO or the health agencies of the US, Canada or Australia, were the first to be imitated (Proofpoint Threat Research Team, 2020). Other targets were the official government pages of France, the UK, and Canada. In the scope of their "relief fund" phishing campaigns, malicious actors also spoofed institutions such as the US Internal Revenue Service (IRS), Her Majesty's Revenue and Customs (HMRC) or the City of Westminster City Council in the UK (Proofpoint Threat Research Team, 2020). NATO and the UN were also imitated in some campaigns (Arsene, 2020) as well as Switzerland's Federal Office of Public Health (MELANI, 2020).

The second type of targets were a host of online services (e.g. video streaming websites), to which many people turned while at home. One of the main targets was Netflix, which was the subject of a Facebook Messenger campaign that promised two months of free access before redirecting the victim to a fake Netflix login page in order to steal their credentials (Trend Micro, 2020a).

The widespread phishing phenomenon around the coronavirus crisis was particularly abetted by the relatively good quality and availability of ready-to-use templates on various forums (Proofpoint Threat Research Team, 2020). This made it easy for threat actors to quickly create high-quality, malicious web domains to insert into their coronavirus phishing campaigns (Proofpoint Threat Research Team, 2020).

Phishing Scale Indicators

In terms of scale, public reporting varies but overall underlines the "dramatic increase" of malicious phishing campaigns leveraging coronavirus lures, especially in the first couple of months of the pandemic (O'Neill, 2020; Wiggen, 2020). For instance, the cybersecurity firm Barracuda Networks reported that the number of coronavirus phishing emails increased by 667 per cent on its network between the first two months of 2020[20] (Muncaster, 2020d). In mid-April, Google reported that, in just one week, it saw more than 18 million malware and phishing emails related to coronavirus scams on a daily basis that were sent via Gmail alone. These figures are separate from and add to the 240 million daily coronavirus-related spam messages Google reported (Check Point Software Technologies, 2020c; Kumaran and Lugani, 2020; Lyons, 2020). In addition, Google disclosed that in January, it registered 149,000 active COVID-19 phishing websites. In February, that number nearly doubled to 293,000. By March, that number had increased again to 522,000 – a 350 per cent increase since January (Radoini, 2020).

Figure 2: Most frequent coronavirus-related phishing subjects (author; Interpol, 2020b)

Relief Fund	Financial scams offering payment of government assistance during the economic shutdown
Coronavirus Updates and Safety Measures	Health advice and information about vaccines, masks and short-supply commodities like hand sanitizer, made to look like they originated from national or global health authorities
Streaming Sites	Free downloads for technology solutions in high demand, including video and audio conferencing platforms, such as Netlfix
Business and Work Procedures	Critical updates to enterprise collaboration solutions and consumer social media applications
Tracking and Contact Tracing Apps	Free downloads or updates for pandemic tracking and pseudo official contact tracing apps for mobile phones
Investments and Stock Offers	Attractive financial opportunities for various products, including fake treatments, medical equipment or financial transactions relating to retirement savings
Charity and Donation Requests	Call for donations, sometimes in Bitcoins, to fake COVID-19-funds to help the victims, the healthcare workers or development of vaccines

[20] i.e. from 1188 incidents in all of February to 9116 incidents as of 26 March.

In Switzerland , MELANI reported that it was able to identify about 3000 unique phishing sites. It also recorded an increase in phishing attacks on website operators and domains owners in order to gain generalized access data (MELANI, 2020).

Despite this relatively fast increase, some reporting highlights that there was an observable peak in March, with a subsequent drop in April. The peak varied from place to place, for instance in Switzerland, this peak, according to MELANI, was in April before falling in May (MELANI, 2020). According to Proofpoints' threat research team, this was likely due to a combination of saturation for coronavirus payment theme phishing templates and a move towards other coronavirus themes as many one-time payments had been disbursed (2020).

One other indicator of the scale of phishing attempts are domain registrations relating to the coronavirus crisis. These include, for instance, key words such as "coronavirus", "corona" or "COVID-19" but also "relief payment", or "cure". While these domains can be used for other purposes than phishing, impersonation and spreading malware, including for instance misinformation and scams, they are a central element of any phishing campaign. Not all of these coronavirus-related domains were, however, malicious. Many of them are used by official institutions to raise awareness, such as the Center for Disease Control and Prevention (CDC) in the US or the Federal Office of Public Health (FOPH) in Switzerland.

By the end of April, reports by the cybersecurity and hardware company Check Point Software Technologies (2020) estimated that among the 20,000 coronavirus-related domains it had assessed in April, 2 per cent were definitely malicious and 15 per cent suspicious. Interpol published similar estimates for March and rated 2000 out of 116,000 reviewed domains as malicious and 40,000 as high-risk domains (Interpol, 2020b). Despite this low percentage, Checkpoint Software Technologies highlighted that newly registered coronavirus-related domains are still 50 per cent more likely to be malicious than other domains (Check Point Software Technologies, 2020b). In Switzerland, the trend was similar, with an expert from SWITCH, the Swiss foundation managing the .ch and .li domains, underlining "a sharp increase in suspicious activity reports in connection with new domain registrations" (Städeli, 2020).

Unsurprisingly, in terms of scale and evolution, before 2020, only 190 domains using prominent keywords related to the pandemic were registered (Intsights, 2020). This number then soared, in the first months of the epidemic, with a noticeable spike on 12 February when the WHO named the coronavirus disease as COVID-19 (CyberPeace Institute, 2020). According to some estimates, in January alone there were over 1400 registered domains, in February that number increased to over 5000 before topping at least 38,000 (116,000 according to Interpol) by the end of March and over 90,000 in May (Check Point Software Technologies, 2020c; Interpol, 2020b; Intsights, 2020; Trend Micro, 2020a).

Several reports highlight the speed, particularly in March, with which such phishing fronts were created. For instance, the threat intelligence firm RiskIQ reported to have seen "more than 13,500 suspicious domains on 15 March; more than 35,000 domains the next day; and more than 17,000 domains the day after that." (Cimpanu, 2020e). The CyberPeace Institute reported that the total number of newly registered COVID-19-themed domains was around 16,000 on 9 March before doubling over the course of the week (2020). After the peak in March, the number of registered domains gradually slowed down as the focus changed and some mitigation measures were put in place (CyberPeace Institute, 2020). This included, for instance, the domain registrar Namecheap blocking the registration of applications using "coronavirus" in combination with the term "vaccine" (CyberPeace Institute, 2020).

In terms of subjects and focus, one can discern an evolution as the months passed by (Check Point Software Technologies, 2020d). At the beginning of the outbreak – when everybody was eager to track the global spread and understand the symptoms – a great number of these domains were related to live maps and COVID-19 symptoms. Towards the end of March, the focus turned to relief packages and stimulus payments as various economic and financial plans were deployed in several countries. Then, as several countries eased their lockdowns, domains related to life after the coronavirus became more common, as well as domains about a possible second wave of the virus. Throughout the pandemic, domains related to tests kits and vaccines have remained very common, with slight increases as time wore on (Check Point Software Technologies, 2020d).

Linked to malicious domains, another phishing indicator is the creation of fake URLs associated to the coronavirus crisis. These fake URLs, spoofed to look like legitimate ones, are normally used alongside malicious domains to inject malware once opened. In terms of scale, Proofpoint reported that in April over 300,000 malicious URLs had been created (Proofpoint, 2020). The computer security firm McAfee, meanwhile, reported that in the first 13 weeks of the pandemic it saw the number of fake website increase from 1600 to over 39,000 (McAfee, 2020b). In terms of efficiency, the cybersecurity firm TrendMicro (2020a) reported that between February and the end of March, it had recorded over 48,000 hits of malicious URLs related to COVID-19 on its network.

As such, these indicators tend to portray a sharp rise in volume and speed of COVID-19-related phishing attacks, many of which were opportunistic, leveraging pre-existing templates and replacing other types of non-

COVID-19-related malicious actions. However, as mentioned in section 1.3, these attacks have not been significant when compared to the overall number of attacks.

2.2.5 Malware

Linked to all the above-mentioned phishing activities, the coronavirus crisis has also been an excellent opportunity for malware distribution, notably through malicious links or attachments. According to a TrendMicro report, in the first three months (Q1) of 2020 alone, over 737 malware threatsrelated to coronavirus – many repurposed – were detected (Trend Micro, 2020a). Proofpoint researchers in late April identified over 200,000 malicious attachments with coronavirus themes across over 170 campaigns (Proofpoint, 2020). Both of these numbers have since increased. Among the various types of malware, two overarching types can be discerned, namely disruptive malware (e.g. ransomware or data wipers) and data harvesting malware (e.g. Trojans or crypto miner).

Disruptive Malware: Ransomware

Among disruptive malware, the most prevalent form found in the wild was ransomware, with ransomware-as-a-service increasingly becoming an established criminal enterprise. Indeed, a report by the cybersecurity company Coveware notes that ransom demands in the first quarter of this year increased by 33 per cent compared to the last months of 2019 (2020). Operationally, these come later in the attack chain and usually infect the victim's system via email attachments, links, or through compromised credentials obtained with coronavirus lures or other techniques, such as RDP brute force attacks (Interpol, 2020a; Khan et al., 2020).

Overall, malicious actors, such as the *Maze Ransomware group* (aka *TA2101*), have particularly taken advantage of educational, medical, and public institutions, as well as businesses – often targeting organizations operating under stress – to maximize profits. Many criminals seemed to have been optimistic that these institutions would be more prone to indulge their crime and pay the ransom due to this external pressure. This appears to be supported by EUROPOL, which noted that the activation and payment time for ransomware have diminished (Europol, 2020a).

Among the myriad of ransomware campaigns observed, some deserve more spotlight than others for their blatant leveraging of the coronavirus, their targeting, and their impact. The first being the new ransomware variant dubbed "*CoronaVirus*." This particular strand was uploaded and spread through a fake *Wise Cleaner* – a system optimization software – website. The victims, which included the two Czech hospitals mentioned above, were lured to download the fake setup file from the site. Once the victim installed the software, this malware acted as a regular ransomware, stole a password, and encrypted the data (Khan et al., 2020). However, it also installed the password-stealing Trojan *Kpot*, which purloins "cookies and login credentials from web browsers, messaging programs, VPNs, email accounts, gaming accounts, and other services" (Abrams, 2020b; Trend Micro, 2020a). As such, this campaign seems to be only one among others that go beyond traditional ransomware activities and simultaneously steal information, potentially to facilitate a later attack or extortion (Abrams, 2020b).

A second noteworthy ransomware campaign during this pandemic concerns a tweaked (in this case less detectable) variant of the famous *Netwalker* ransomware (formerly *Mailto*). According to Malwarehunterteam, it has used coronavirus lures to target various enterprise and government agencies (Abrams, 2020c). These notably included the two widely reported attacks against the Toll Group and the Champaign Urbana Public Health District (CUPHD) in Illinois (Abrams, 2020c).

Another one is the *fuckunicorn* ransomware, which was observed in a typo-squatting campaign[21] focused on the Italian Federation of Pharmacists (IFP), which was a key information provider on the pandemic in Italy. Specifically, the ransomware campaign crafted a malicious website imitating the IFP site, along with a slight variation of the IFP site's domain name. Similar to other prevalent attacks, users are lured into downloading the ransomware that masqueraded as a pandemic "dashboard tracker" (Walter, 2020).

A last noteworthy example is the *Winlocker* ransomware, which was adapted from its 2019 form to display a lock screen with a coronavirus image while repeatedly/ annoyingly saying "coronavirus" demanding a password to regain system access (TrendMicro, 2020a).

As mentioned, numerous others have been observed in the wild. Among the most prevalent we find the *Lockbit, CERBER, Wannacry, Sodinokibi, Cryptolocker, NanoCore* and *Ryuk* ransomware (Interpol, 2020b, 2020a; Intsights, 2020; MELANI, 2020). As such, most of the ransomware observed in the first half of 2020 seems to come from pre-existing strands, leveraged by well-known actors or widely available on the markets. Nonetheless, ransomware – alongside phishing and credential stuffing – has been the emblematic/prevalent threat during this pandemic. As mentioned above, the *modus operandi* of threats actors leveraging these types of attacks has evolved and

[21] Also known as *URL hijacking*, it is a form of cybersquatting (sitting on sites under someone else's brand or copyright) that targets Internet users who incorrectly type a website address into their web browser (e.g., "Gooogle.com" instead of "Google.com") (McAffee, 2013).

become more reckless and sophisticated – i.e. targeting critical infrastructure, engaging in double extortion and shortening penetration to activation time.

Disruptive Malware: Data Wiper/ MBC Rewriter

Another type of observed disruptive malware have been boot record rewriters, which wipe a computer's master boot record (MBR) (Cimpanu, 2020f). The information security journal ZDNet has identified at least five malware strains that use a coronavirus theme and are geared towards destruction, rather than financial gain. One of them, which used the name "COVID-19.exe", first showed an annoying window that users cannot close as Windows Task Manager is disabled all the while it was rewriting the master boot code (MBC) (Cimpanu, 2020f). A second strain posed as the coronavirus ransomware mentioned above before actually rewriting the MBC.

Furthermore, Malwarehunterteam also found two data wipers. The first was spotted in February and used a Chinese file name to target Chinese users. It, however, remains unclear whether this first case was actually distributed in the wild or just a test. The second data wiper was spotted in early April (Cimpanu, 2020f).

Data Harvesting Malware: Trojan

In terms of data harvesting malware, the majority of cases reported during the pandemic fall within the Trojan malware family. Many of these lured their victim – in all types of sectors – with WHO or COVID-19 lures. Examples include the *Formbook,* the *Hancitor,* and *Gracewire* Trojans, which were installed by the *Guloader* and *Get2Loader* malicious downloader, respectively (Abrams, 2020d; Cybersecurity & Infrastructure Security Agency and National Cyber Security Centre, 2020; McAfee, 2020b). Trojans can take many forms, such as (1) remote access Trojans (RATs), (2) banking Trojans, and (3) information stealing Trojans.

(1) RATs are often used for creating and maintaining botnets – and thus used for DDoS attacks – but also uploading files to an infected device, executing scripts, taking screenshots, harvesting keystrokes, stealing bitcoin wallets, and collecting browser cookies and passwords (CERT-MU, 2020). During this pandemic, one of the most reported campaigns included the *Remcos* Trojan, which spread in late March through a phishing campaign around loans in the retail and SME sectors as well as the Philippines' Bureau of Customs (F and Scholten, 2020; Intsights, 2020; McAfee, 2020b). Other campaigns included the *Crimson RAT*, the *Koadic RAT,* the *Warzone RAT,* the *Nanocore RAT, IceID,* or the *BlackNET RAT*. The latter was disseminated through two simple websites promoting fake applications; aptly called "antivirus-covid19" and "corona-antivirus" (Degrippo, 2020b; Intsights, 2020; McAfee, 2020b; Platt et al., 2020; Threat Intelligence Team, 2020; Walter, 2020).

One particularly active coronavirus-related campaign involved the well-known *AgentTesla* spyware, which collects information about the actions of its victims by recording keystrokes and user interactions. This new medium-sized campaign posed, among others, as the head of the WHO, claiming to have found a "solution for COVID-19". Mostly present in the United States, it primarily targeted the manufacturing industry but also construction, transportation, healthcare, automotive, energy, and aerospace companies (Proofpoint, 2020).

(2) Banking Trojans, meanwhile, tend to try to steal credentials to illegally obtain money. Among the different Trojan families active during this pandemic, reports have highlighted the use of the *Trickbot* banking Trojan in a variety of coronavirus-related campaigns. In one example, emails targeted Italian users with a document purporting to be information related to COVID-19 but instead executed the Trojan (Abrams, 2020e; Cybersecurity & Infrastructure Security Agency and National Cyber Security Centre, 2020).

Another noteworthy and active banking Trojan has been the *Zeus Sphinx* malware (aka *Zloader* or *Terdot*), which after years of lying dormant, has been resurrected to capitalize on the pandemic (Osborne, 2020). According to IBM X-Force, this campaign was launched in March and focused on government relief payments, notably in the UK, Australia, Brazil, and the US (Gandler and Kessem, 2020; Osborne, 2020).

A last family that has been widely reported on has been the *Emotet* (aka. *Geodo* or *mealybug*) Trojan. According to antivirus firm McAfee (2020), several campaigns used COVID-19-themed phishing (e.g. on treatment and research) to deliver the Trojan. They notably affected China and Japan in the early months of the pandemic and in particular targeted the healthcare sector (Trend Micro, 2020b).

3) Information-stealing Trojans are designed to gather information from a system, such as logins, usernames, passwords, keystrokes (TrendMicro, n.d.). One particularly saliently reported campaign has revolved around the relatively new *Oski* info stealer malware. This malware was propagated through a fake information app – the "COVID-19 Inform App" – allegedly developed by the WHO. Cybercriminals were able to hijack routers and change Domain Name System (DNS) settings to redirect victims to attacker-controlled sites promoting the fake coronavirus information apps (Arsene, 2020b; Cimpanu, 2020g; Trend Micro, 2020a). These criminals mainly targeted D-Link and Linksys products using brute-force attacks to guess the admin password of targeted routers (Cimpanu, 2020g). The campaign, which allegedly started on 18 March, affected over 1000 individuals in the space of one week (Arsene, 2020b). According to cybersecurity company Bitdefender, it mostly affected targets from the US,

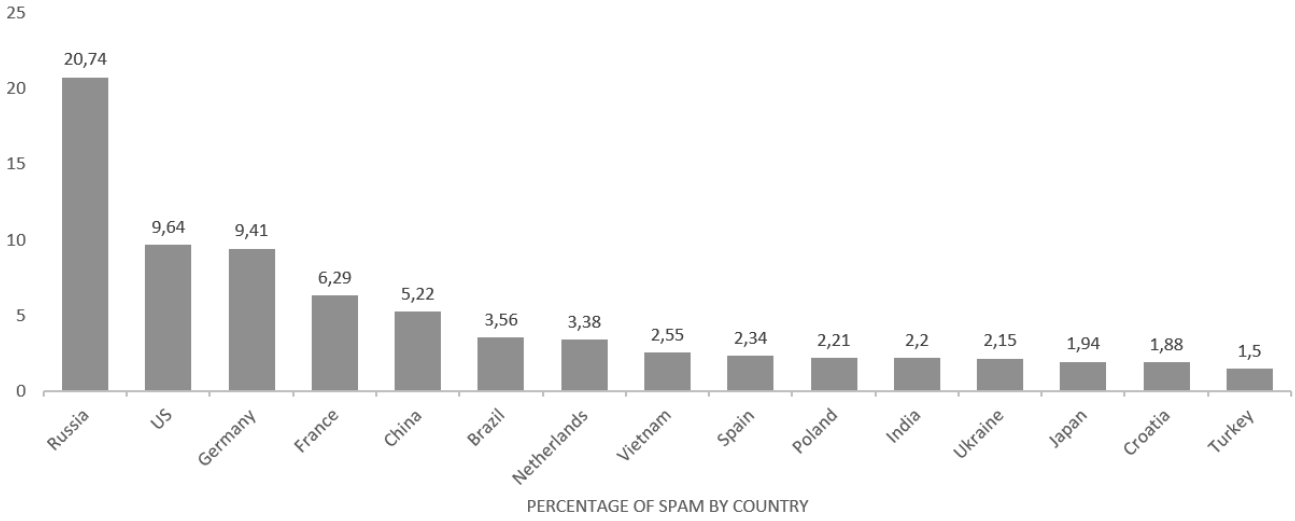
Germany, and France, which were at the time among some of the countries most affected by the coronavirus outbreak (Arsene, 2020b).

Cybercriminals have also been active in spreading a new variant of the *HawkEye Reborn* and *Lokibot* malware. The former, which has been revamped with extended information-stealing capabilities, has been

Data Harvesting Malware: Crypto Miners

Another type of data-harvesting malware active during the early months of this pandemic has been the *Lemon Duck* crypto miner – first spotted in 2019. In an ongoing campaign first observed in March, spammers aimed to spread the malware through coronavirus-themed emails

Figure 2: Sources of spam by country in Q1 (Scherbakova et al., 2020)



used to target the retail sector through the intermediary spam that purports to be an "alert" from the Director-General of the WHO (Brumaghin and Unterbrink, 2020; Seals, 2020). Anecdotally, it has been reported that the owner, called MoonD3v, apparently auctioned off this malware after he was diagnosed with COVID-19 (Blueliv, 2020).

Lokibot has also been distributed using a WHO-spoofing spear-phishing campaign, this time ironically pertaining to misinformation around the pandemic (Saengphaibul, 2020). It is a prolific Trojan infamous for being simple, effective, and cheap (it used to be sold for as little as 300 USD) (Montalbano, 2020). Since it was first detected, the spear-phishing campaign has gone global, with Turkey, Portugal, Germany, Austria, and the United States showing the highest incidents, while Belgium, Puerto Rico, Italy, Canada, and Spain were also affected (Montalbano, 2020; Saengphaibul, 2020).

The last highly reported scheme revolved around the interactive coronavirus dashboard maintained by Johns Hopkins University. Hackers took advantage of it in March and embedded a fake but accurate version of the dashboard with the java-based *AZORult* Trojan (Alfasi, 2020; Krebs, 2020d). The kit was notably sold on several Russian-language cybercrime forums for 200 to 700 USD (Intsights, 2020).

with weaponized attachments (Trend Micro, 2020c). Once a machine had been compromised, the users' Microsoft Outlook account sent emails with malicious attachments to their contacts (Trend Micro, 2020c). Incidents have been reported in China, Bangladesh, Hong Kong, Egypt, and Indonesia, mostly affecting the clothing industry, real estate, and health, electronics as well asshipping/logistics companies (Trend Micro, 2020c).

Later reports have also revealed that *APT32* (or *Ocean Lotus*), has been hiding behind a crypto miner to target French and Vietnamese government and private sector entities (Lakshmanan, 2020).

2.2.6 Business Email Compromise (BEC)

Amid the plethora of coronavirus-related phishing attacks across the globe, one type of threat that has also seen some adaptation is business email compromise. The scam works by convincing or tricking the targets – e.g. by using spoofed supplier or client addresses – into making transactions to an intruder who poses as an employee working in the same company (Khan et al., 2020). Indeed, some researchers, the FBI, Europol, and other law enforcement agencies have reported that BEC scammers have increasingly been using COVID-19 as a hook to reinforce the sense of urgency (FBI National Press Office, 2020; Peterson, 2020; Trend Micro, 2020a). In terms of scale, no definitive figure exists. By way of orientation, according to the security company

Symantec, BEC attacks targeted more than 30,700 organizations in the first quarter of 2020; however, not all were approached with a coronavirus lure (Symantec, 2020).

One of the earliest reported BEC campaigns leveraging the pandemic was perpetrated by the known cybercrime group *Ancient Tortoise*. This campaign is believed to be an adaptation of the previous attacks the group launched (Gatlan, 2020; Trend Micro, 2020a). Operationally, the group first targeted the bank accounts before using the customers' details to send them emails to inform customers of a change in banks and payment methods due to the coronavirus crisis (Gatlan, 2020; Khan et al., 2020).

In the US, the FBI also provided the following two telling examples of BEC (FBI National Press Office, 2020). In the first, a US bank received an email allegedly from the CEO of a company, who had previously scheduled a transfer of one million USD, requesting that the transfer date be moved up, and the recipient account be changed "due to the Coronavirus outbreak and quarantine processes and precautions" (FBI National Press Office, 2020). In the second, a bank customer was emailed by someone claiming to be one of the customer's clients in China. The client requested that all invoice payments be changed to a different bank because their regular bank accounts were inaccessible due to "Corona Virus audits." The victim sent several wire transfers to the new bank account at a significant loss before discovering the fraud.

2.2.7 (Mal)Spam

Spam, be it by email or text, is one of these nuisances – and threats when weaponized – that have existed since the Internet's inception. Cluttering both the Internet and most email inboxes, spam accounts for a massive volume of emails sent every day and pertains to as many subjects as one can think of. Whether in a moment of relative calm or an emergency situation, spam has always been used on a very large scale by malicious actors to advance their cause and interests. The current pandemic is no exception.

In the current epidemic situation, coronavirus-related spam has been observed on a very large scale sent to users as early as February 2020 (Khan et al., 2020; TrendMicro, 2020a). Indeed, TrendMicro reported that in the first quarter of 2020 it had observed nearly one million spam messages – mostly in the US – related to the pandemic, with a 220 per cent increase between February and March (Trend Micro, 2020a). Google, meanwhile, reported that in early April its Gmail networks were seeing over 240 million coronavirus spam messages daily, without accounting for an additional daily 18 million phishing and malspam emails (Kumaran and Lugani, 2020).

According to the cybersecurity company Kaspersky, in first quarter of 2020, Russia was the first country by the amount of outgoing spam. It was followed by the US, Germany, France, and China (traditionally in the top 3) (see. Figure 1.) (Shcherbakova et al., 2020).

Examples of (mal)spam are legion, characterized by different degrees of sophistication (and typos). Among these cases, the themes and lures are similar to those mentioned above regarding phishing (e.g. WHO spoofing, COVID-19 remedies, etc.). For instance, one very common example includes spammers pretending to be the WHO by spoofing an official email address by using the domain name extension ".int" instead of the official ".org" and asking for donations in bitcoins (WHO, 2020b). Another one impersonated the Colombian government with a weaponized attachment disguised in the form of a map of infected neighborhoods (Szocs and Bejean, 2020). With large parts of the population staying at home and ordering food or other goods online during the initial lockdown put in place in many countries, malspammers have also sent emails pertaining to shipping transaction, either about postponement due to the spread of the disease or messages that provided a shipping update (Shcherbakova, 2020; TrendMicro, 2020a)**.** Spam has also been used to spread and exploit fear, paranoia, and naivety in whimsical ways. For instance, one spam campaign pushed out a video ad for a bogus doomsday survival course in the wild (F and Scholten, 2020).

As the pandemic progressed, researchers have also observed a gradual evolution in the type of (mal)spam campaigns out there. According to Symantec researchers, the first wave, which arose in early March, comprised mostly of coronavirus-related (mal)spam and phishing emails (Thaware, 2020a). These messages distributed a variety of malware (discussed in section 2.2.4), from generic to custom-built Trojans, information stealers, and malicious downloaders. Still, according to Symantec, there was a sharp uptick in the number of malicious emails (in the US) on 16 March, with a surge of spam campaigns focused around selling face masks, medical equipment, immunity oil, and other products related to the coronavirus outbreak (Thaware, 2020a). This increase closely corresponded with the rise in the number of COVID-19 infections recorded in Europe and the US as well as a sudden shift in the US public perception of the related risks (e.g. looting and hoarding in some regions) (Thaware, 2020a).

In the following weeks, a second wave of spam emails took over in the form of so-called snowshoes spam. It remained the predominant/favorite type at least until May (Thaware, 2020a, 2020b). These campaigns tended to appear with heavy randomization in the header fields to avoid detection and come in large batches in a short period of time. These spam volleys have used a myriad of topics and themes, such as "Elon Musk Reveals How to Profit from coronavirus" and the promotion of a "Touch Free Body Thermometer" (Thaware, 2020b).

2.2.8 Distributed Denial of Services (DDoS)

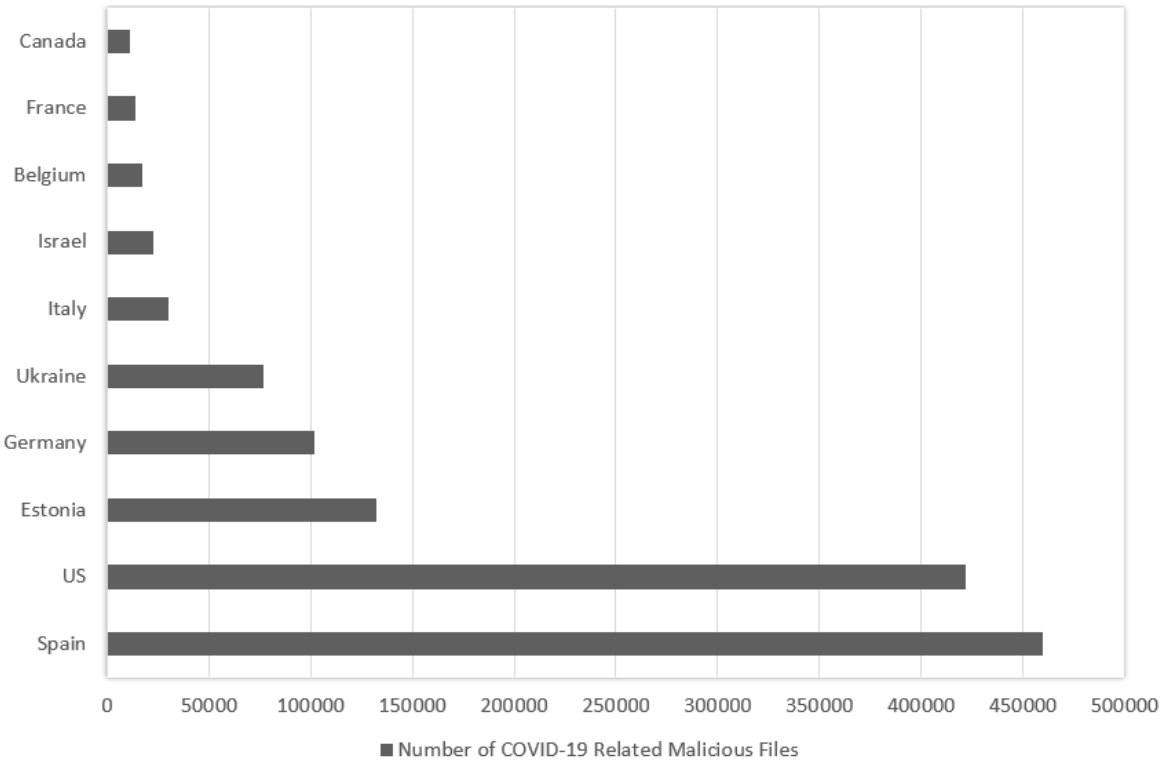
In the context of the pandemic, the number – and in some cases the severity – of DDoS attacks has also increased worldwide (Europol, 2020d; Hope, 2020a; Nexusguard, 2020). Indeed, according to the cybersecurity firm Nexusguard, DDoS attacks within the first quarter of 2020 increased by 542 per cent compared to the last quarter of 2019 and by 278 per cent compared to the same period in the previous year (Nexusguard, 2020). According to Kaspersky, in Q1 and Q2, the average number of attacks per day increased by almost 30 per cent compared to the previous reporting period (Kupreev et al., 2020). A similar trend has been confirmed by the security firms Cloudflare and Netscout, which noted that the increase grew in parallel to the pandemic – i.e. with a big spike between 11 March and 11 April 2020 (over 864,000) (Dobbins and Hummel, 2020; Yoachimik and Singh, 2020).

On top of that, researchers at Kaspersky added that the increase in DDoS attacks from Q1 2020 and Q2 2020 grew about 5 per cent (Zurier, 2020). Despite being a small rise it is unusual as past years trends have seen Q1 being lower than Q2. In addition, compared to the same period of Q2 2019, DDoS attacks grew more than threefold (Zurier, 2020). Moreover, they also noted that in Q1 2020, the average duration of DDoS attacks also grew; with attacks lasting 25 per cent longer than in Q1 2019 (Zurier, 2020).

In terms of attack geography, trends in Q1 and Q2 are very similar. The top five places in terms of both the number of targets and the number of attacks were occupied by China (approx. 61 per cent), the United States (approx. 19 per cent), Hong Kong, China (approx. 6 per cent), South Africa (approx. 1.5 per cent) and Singapore (approx. 1 per cent) (Kupreev et al., 2020). Switzerland, meanwhile, did not record any significant increase in DDoS attacks during the first half of the year (MELANI, 2020).

Compared to previous DDoS attacks that were conducted against public-facing resources of companies, attacks during the pandemic have targeted internal infrastructures of companies, such as their VPN or email servers – often obfuscating more malicious and harmful infiltrations of an organization's resources (Burt, 2020).

Figure 3: Number of COVID-19-related malicious files for Q1 and Q2 (McAfee, 2020c)



In terms of targets, one well-reported DDoS attack was the – supposedly state-sponsored – 15 March DDoS attack that affected and attempted to disrupt the US Department of Health and Human Service's online services and its pandemic response activities (Stein and Jacobs, 2020). According to various official sources – e.g. Health and Human Services Secretary Alex Azar – the attack was unsuccessful (Stein and Jacobs, 2020). As a side note, various networks and companies, such as T-Mobile, Verizon, A&T, and Sprint thought they were being targeted by a coordinated DDoS attack in mid-June. The attack, however, was later debunked and due to a misconfiguration on T-Mobile's end (Raywood, 2020).

Amazon Web Services (AWS) also reported the mitigation of a 2.2 terabit-sized DDoS strike in February,

which would have rendered thousands of their hosted clients useless for an unknown time period (AWS Shield, 2020). Despite not being the only victim of the attacks, its size was nonetheless highly unusual and represented a 44 per cent increase in any data volume previously recorded on their network (AWS Shield, 2020; Bytagig, 2020).

AWS was not the only one to have experienced such a major attack. Indeed, in Europe, the network host Akamai discovered and thwarted a DDoS attack attempt against a European bank in June. Specifically, the strike attempted to overload the network with over 800 million packets per second (PPS). This was not the traditional form of DDoS attack, which usually strikes with BPS (bits per second) attacks, targeting, and overwhelming networks. A PPS-approach instead seeks to drain network resources (Bytagig, 2020; Emmons, 2020). In addition, network provider Akamai also reported that it had thwarted a 1.44 Tbps attack in the first week of June 2020 (Emmons, 2020).

This is not the only unusual activity reported; researchers from the cybersecurity provider Nexusguard also discovered various abnormal traffic patterns, including small-sized, short attacks known as "invisible killers" which most ISPs overlook thus allowing the attackers to cut through to online services and cause disruption (Hope, 2020a; Nexusguard, 2020).

A last type of DDoS attacks observed during the coronavirus pandemic has been "ransom DDoS" or "extortion by DDoS", where threat actors threaten an organization with a massive DDoS attack if it does not pay up. These types of attacks had subsided in the past years but have been on the rise again – particularly since July/August (Muncaster, 2020e; Radware, 2020). Threat actors, such as the *Armada collective* and *Fancy Bear* – and some copycats –targeted businesses in the e-commerce, finance, and travel sectors in North America, Asia pacific, Europe, the Middle East, and Africa.

***

As mentioned earlier in section 1.2.2, in the first six months of 2020 the scale, sophistication, and *modus operandi* of certain cyber threats have evolved to adapt to the pandemic environment. This notably includes the (re-)emergence of double extortion ransomware, of old malware such as *Zeus*, stronger DDoS attacks as well as increasing attacks against cloud services and VPNs. However, as previously for the actors, the types of cyber threats – at least those exploiting COVID-19 – are more of the same. Most of the detected malware groups were active and known before the pandemic and little innovation in terms of actual attack techniques, tools and procedures has been observed. Instead, the attacks were merely re-adapted to fit the pandemic and exploit the situation to the maximum.

2.3 Distribution and Types of Targets

Concurrent with the large volume of coronavirus-related cyberattacks, the number, distribution, and type of targets affected were similarly large and diverse. "Targets" is a large category referencing anyone or anything being affected by cyberattacks. As such, it can be divided into at least three different levels of granularity, ranging from the country level, down to sectors, and eventually individual actors.

The following paragraphs describe, exemplify, and tentatively quantify these levels, namely the states, sectors, and types of individuals that were primarily targeted by coronavirus-related cyberattacks. As a caveat, quantifying and qualifying targets is, due to incomplete or lacking data, often a delicate affair and the following sections only aim to provide a general indication as to the general trend during the first six months of 2020. In addition, the chosen set of affected sectors is far from exhaustive and only aims to highlight those most affected.

2.3.1 Geographical Distribution of Attacks/ Targets

Understanding the geographical distribution of cyberattacks is essential to provide a more complete view of the cyber threat landscape – differentiating between perceptions of threats and actual threats. It allows to identify those regions or countries most affected and thus at risk from certain types of attacks; thus helping policymakers to put in place the necessary counter-measures to enhance their cybersecurity. Additionally, it also helps to ascertain different regional trends and patterns in adversarial behavior.

As such, in terms of the geographical distribution of the targets, researchers have observed – similarly to the pandemic itself – the truly global reach and dynamic nature of coronavirus-related cyberattacks. Perhaps obvious, but these cyberattacks seem to have closely followed the spread of the coronavirus, mostly targeting countries that had started suffering an increase in COVID-19 cases (Arsene, 2020a; Guirakhoo, 2020b). In March, for instance, researchers at Proofpoint observed that several countries were particularly affected, such as Italy, the Czech Republic, Japan, the UK, Spain, France, India, Romania, Thailand, the United States, Canada, Australia, and Turkey (Arsene, 2020a; F and Scholten, 2020). At the time, all of these countries were seeing a very steep increase in the number of cases and hospitalizations due to COVID-19. These connections further highlight the continuing adaptation capacity of threats actors already underlined in section 1.3

Regarding the extent to which these countries were affected, one can for instance turn towards anti-virus statistics for a glimpse of the reality. According to Kaspersky and its email anti-virus, Spain had the highest number of malware "trigger events" in Q1 2020 and

accounted for 9.66 per cent of all users of Kaspersky's security solutions who encountered email malware worldwide. Second place went to Germany (8.53 per cent), and Russia (6.26 per cent) ranked third (Shcherbakova et al., 2020).

According to McAfee's COVID-19 threat dashboard (see figure 4)[22] that tracks COVID-19-related malicious file detections, Spain remained the most affected country during Q1 and Q2, with about 460,000 malicious detections (at the time of writing). The leaderboard afterward however is different (see figure 2) (McAfee, 2020c). Incidentally, the disclosed incidents targeting the US in Q1 2020 rose 61 per cent compared to the previous quarter (McAfee, 2020b), making it one of the countries most-hit by coronavirus-related cyberattacks – after Spain.

While many of the COVID-19-related cyber threats have been shared across the world (e.g. phishing or ransomware), not all countries were affected to the same extent and by the same threats – reflecting both the adaptation capacity of threat actors but also different regional trends – depending on regional capacity, opportunities, or financial interests. In that regard, a number of regional cybercrime trends can be highlighted. According to the Global Assessment Report on COVID-19 related Cybercrime published by INTERPOL's Cybercrime Directorate,[23] Europe was particularly targeted, most notably by (credential) phishing, spoofing of official websites, and ransomware against critical infrastructure operators (Interpol, 2020b). In the Americas, countries were particularly affected by COVID-19-based phishing and fraud, which included the use of remote access hacks, ransomware against SMEs (e.g. *Lockbit*), as well as child exploitation. African countries reported increased cyberattacks against online payments, COVID-19-related phishing, and extortion. Countries in Asia and the South Pacific reported fraud and phishing campaigns as well as the illegal online sale of fake medical supplies, drugs and personal protective equipment. The Middle East and North African regions were also hit by an increasing number of phishing, online fraud, malicious domains and scams. All regions reported mis- and disinformation on social media. As highlighted in Europol's latest Organized Crime Threat Assessment (2020d), none of these threats were in themselves new to the different regions. In most cases, COVID-19 has only amplified the intensity of some pre-existing threats (e.g. phishing, ransomware, and scams) – while diverting effort and resources from others.

2.3.2 Most Targeted Sectors: Public, Health, Education, and Financial Sectors

According to public reporting, cyber malicious actors have spared no one and no sector with their coronavirus-related cyberattacks. Indeed, sectors from retail to energy as well as construction or transport have been targeted and affected, directly or indirectly, by these attacks. However, some sectors need to be highlighted as to the intensity with which they were (and probably continue to be) targeted and the (potential) impact these attacks have had. These are the public sector, the health sector, the education sector, and the financial sector.

Public Sector

The public sector, particularly those entities related to the crisis response, such as task forces or health agencies, have been continuously targeted by threat actors during this pandemic, whether for espionage, disruption, or profit.

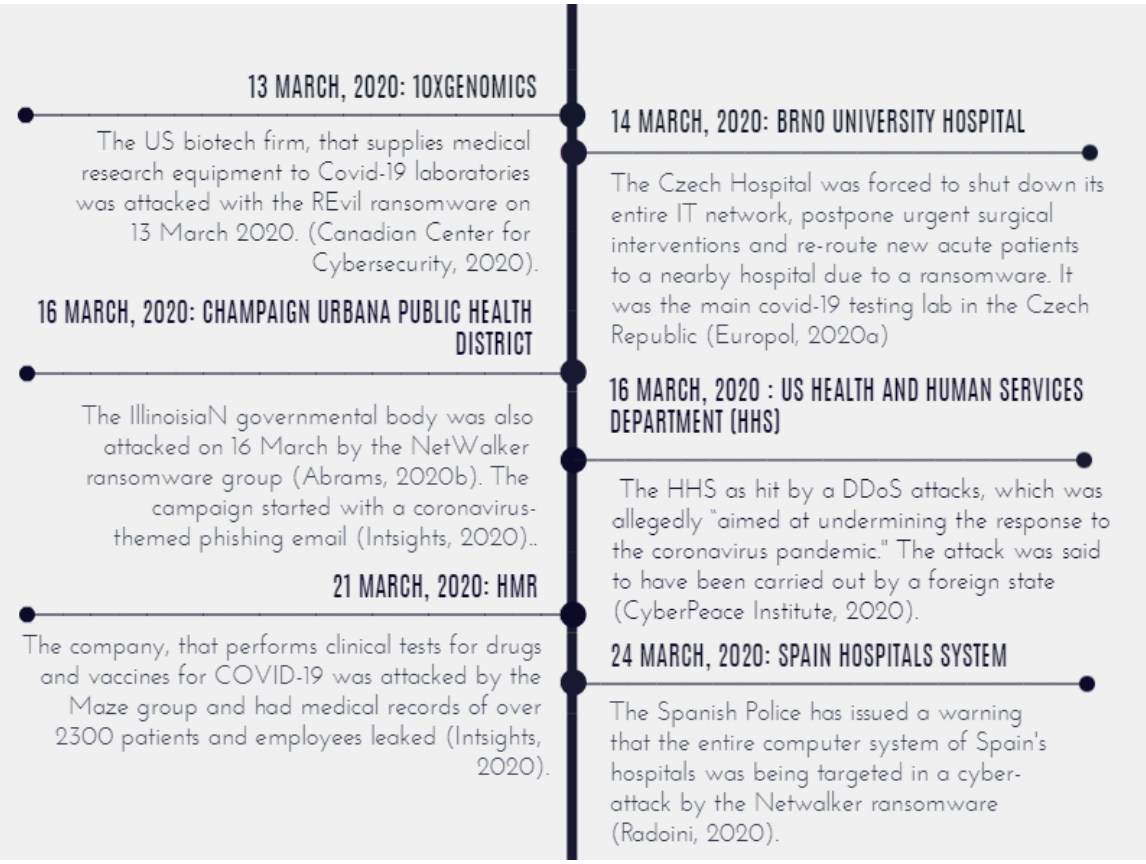
According to McAfee's threat report, incidents detected in the public sector during the first quarter of 2020 increased by 73 per cent – compared to the previous quarter (McAfee, 2020b). While not globally representative, this trend is illustrated in new data found in the Australian Cybersecurity Strategy 2020; in the past year – from Q3 2019 to Q2 2020 – Australia's governmental and public entities were targeted in 35.4 per cent of the incidents its cybersecurity center responded to. Organizations classified as critical infrastructure are second with 35 per cent (Australian Government, 2020).

Among the many types of attacks, many of which are opportunistic ransomware, scams or DDoS attacks (e.g. HHS case), one notable trend includes attacks against the new medical equipment procurement structures that have been developed to respond to the outbreak (Zaboeva, 2020). IBM's X-Force Incident Response and Intelligence Service uncovered and documented a widespread campaign targeting approximately 40 critical organizations in Germany in an effort to disrupt operations and extract sensitive information on their activities. Spear-phishing emails were sent to over a hundred high-level executives at the targeted organizations, which included an unnamed German corporation tied to the procurement of personal protective equipment (Walter, 2020).

[22] The data comes from McAfee's Advanced Programs Group (APG). The dashboard is constantly updated and the numbers indicated were those that had been reported at the time of writing in mid-July 2020.

[23] Conducted from April to May 2020 with 48 out of 194 member countries responding to the Survey and 4 out of 13 private partners contributing their data to the report.

Figure 4: Timeline of major cyberattacks against healthcare infrastructure in March 2020 (author's design)



Health Sector

The healthcare sector has also been under stress and threat both physically (i.e. overwhelmed with patients) and in cyberspace. Indeed, since the start of the pandemic hackers have relentlessly targeted networks, endpoints, and IoT devices of healthcare organizations, hospitals, and clinics, pharmaceutical institutions, and distributors of medical equipment. These have led to considerable disruption and at least one fatality[24] (Sara Coble, 2020). This activity reached such levels that public authorities (e.g. in the UK and the US), international organizations (e.g. the International Committee of the Red Cross), NGOs (e.g. the CyberPeace Institute) and (former) political leaders across the world have made several public calls to stop such attacks.

A number of high-level cases have been reported across the world, affecting countries such as the UK, US, France, Italy, Portugal, Spain or the Czech Republic.[25] Figure 5 provides an overview of the main attacks during the month of March, which recorded a peak of cyberattacks against the healthcare sector. In terms of numbers, the threat intelligence firm Recorded Future has catalogued 26 ransomware attacks against healthcare providers in the US in Q1 and Q2 2020, with attacks being up for every month in year-on-year comparisons (Liska, 2020b). In Europe, those numbers appear to be on the rise as well (Liska, 2020b).

In addition to being the target of media, governmental and individual attention pertaining to the pandemic, the WHO has also been the target of a very high number of cyberattacks. According to its own CISO, Flavio Aggio, since the pandemic began, the cyberattacks against the WHO have increased at least fivefold (WHO, 2020a). Among the campaigns that have received most media coverage one finds the aforementioned one attributed to *DarkHotel*, which, among other things , registered a fake WHO email address and website in March after several failed attempts to steal employee credentials (Intsights, 2020). Another attack resulted in some 450 active WHO email addresses and passwords being leaked online along with thousands belonging to others working on the response to the novel coronavirus (WHO, 2020a).

[24] This incident, which happened outside of the timeframe analyzed for this study, in September 2020, saw the Düsseldorf university clinic fall victim to the crypto locker DoppelPaymer, which has since been linked to a Russian threat actor. As a result, the hospital had to divert patients, one of whom was searching urgent care which the digitally affected clinic was unable to provide, leading to her death.

[25] For a greater overview of all (not only cyber-related) security incident against the healthcare sector see the Safecare project.

In addition, medical research centers – notably working on a possible vaccine – have also been the target of cyberattacks. This includes a set of supercomputing centers across Europe, some of which were involved in projects related to the coronavirus, and whose disruption might have impacted or delayed research. The extent to which these incidents are correlated remains uncertain, though reports by media outlets and cybersecurity companies have speculated that they are (GreAT, 2020b). The British supercomputing center ARCHER, the German based bwHPC, and the Swiss National Supercomputing Center at the ETH Zurich all were affected by security events caused by intrusion attempts in early May. According to an alert made by the European Grid Infrastructure CSIRT – which studied two of the incidents – these were targeted by crypto-mining malware for CPU mining purposes (EGI CSIRT, 2020).

Education Sector

As for many businesses, many (often unprepared) educational institutions were taken aback by the pandemic and had to quickly adapt their logistics to offer continuous learning to their pupils. As a result, many have resorted to various online tools such as Zoom. As mentioned earlier, due to their widespread use these solutions were particularly targeted by different threat actors, whether for cyberespionage, cybercrime or simply disruption. Regarding the latter, a number of Zoom bombings of classes or PhD defenses have been reported.

In addition to the targeting of educational online tools (and their inherent vulnerabilities), the educational sector has also been the victim of a considerable amount of spear-phishing attacks. These were driven, in part, by the constant exchange of and need for information by the faculty, staff, professorial and student bodies on the pandemic, the logistics and future plans (Arsene, 2020a).

Examples include the *Formbook* campaigns, which have been targeting educational institutions via phishing messages with a trojanized application for teachers (Walter, 2020).

The success of these phishing attempts seemed to have been reinforced by the fact that many educational institutions do not have strong cyber awareness, logistics, or practices. For example, according to the security firm Tessian, 40 per cent of the top 20 US universities are not using domain-based message authentication, reporting and conformance (DMARC) records at all. The remaining 60 per cent have implemented DMARC but have not set up policies to "quarantine" or "reject" any emails from unauthorized senders using their domains (Barth, 2020). As a result, many emails and domains can be spoofed to lure students or employees of a university to a phishing website designed to steal credentials or trick victims into giving away financial information (Barth, 2020).

Financial Sector

As for the education sector, the financial one has also been particularly affected by coronavirus-related cyberattacks, whether due to widespread use of teleworking infrastructure or other types of attacks, such as ransomwares. One emblematic attack has been the *Ryuk* ransomware attack against the international financial technology service provider Finastra in March.

After the health sector, the financial one has been one of the most targeted sectors by ransomware. According to the cybersecurity firm Carbon Black, attacks on financial institutions registered an increase of 238 per cent between the beginning of February and the end of April (Upatham and Treinen, 2020). Similarly, in April, the Financial Services Information Sharing and Analysis Center (2020) identified over 1500 high-risk domains, created on or after 1 January 2020, containing both a coronavirus and financial theme. Many of these were used by malicious actors to install Trojans or phish financial credentials from bank customers across the world. In addition, there has also been an increase in banking call center fraud, where fraudsters impersonate customers or make false insurance claims (Financial Crimes Enforcement Network, 2020).

On top of the financial risks these cyberattacks create for both financial institutions and their clients, the exploitation of critical vulnerabilities has enabled both money laundering and terrorist financing, according to the Financial Action Task Force (FATF, 2020). This is mainly due to the increased misuse of online financial services and virtual assets to move and conceal illicit funds as well as the possible corruption connected with governmental stimulus funds or international financial assistance (Crisanto and Prenio, 2020).

2.3.3 Targeted Individuals

Due to the different nature and rhythms of lockdowns and shifts to remote working (see section 1.1), individuals in general – whether working from home or only staying at home – have been relatively easy targets for threat actors. Particularly those individuals with limited risk awareness, user experience, or online literacy/ competence, such as children and the elderly.

Indeed, one group particularly at risk, vulnerable and targeted were children, many of which found themselves lock-down at home and engaged in considerably more and new online activity, whether for e-schooling or entertainment. In addition, children were more isolated and less supervised than usual while content moderation efforts were weakened (due to remote office) and automated. As a result, children have

been considerably more exposed to threats coming from the Internet, such as file-sharing abuse, inappropriate content, cyberbullying, or the grooming of children for sexual purposes (Radoini, 2020; UNICEF, 2020). This is particularly the case for younger children (i.e. under the age of 13), who might not have been familiar with or prepared for the various social networking tools, many of which were not designed for them and thus lack online safeguarding policies (UNICEF, 2020).

The elderly, many of whom were already gripped by fear and abused offline, have also been particularly targeted and abused online. This vulnerable group that more commonly relies on offline shopping and is less cybersecurity aware, had to adapt and increasingly engage in online activities without supervision or support (e.g. for shopping), making them more exposed to scams, hoaxes, and other cyber threats, whether untargeted or directed at them (Radoini, 2020).

The youth and the elderly are of course not the only victims. Many – if not most – of the victims of cyberattacks belong to the more digitally connected generations. According to a study of COVID-19-related online scams and fraud in Switzerland, the bulk of the victims were between 31 and 50 years old (Soguel, 2020). Meanwhile, according to a study by the cybersecurity firm SentryBay, at least 40 per cent of the UK workforce working from home during the pandemic have been victim or had to face attempts of cybercrime (e.g. phishing) (Canter, 2020). As imperfect and incomplete as these results might be, they only tend to illustrate the extent to which malicious activities have targeted a great deal of the population – particularly those parts of the active workforce working from home.

***

The targets of coronavirus-related cyberattacks echo the various changes in terms of targets laid out in section 1.2.3; namely, that malicious actors have acted opportunistically and targeted countries most affected by the pandemic and that to maximize damage, financial and strategic gains, they have shifted their target sets from individuals and small businesses to major corporations, governments, and critical infrastructure organizations that play a crucial role in responding to the outbreak. These most notably include (but are not limited to) the public, healthcare, and financial sectors as well as academic/education institutions. While such sectors and critical entities have been the targets of attacks in the past, the intensity with which they are now attacked constitutes a qualitative change.

Conclusion

The coronavirus pandemic has affected not only the social and work lives of millions but also the cyber threat landscape. Compared to previous crises, it has generated a set of remarkable and unique societal, technical, logistical, and economic circumstances upon which malicious actors – ranging from amateur cybercriminals to sophisticated state-sponsored threat actors – have capitalized to further their financial and strategic aims. There are three such factors, all of which are likely to endure as we move forward. These factors are:

1. an expanded socio-technical attack surface due to the greater use and dependency on services and applications for telework provided through digital infrastructure in general and cloud infrastructure in particular;
2. an psycho-informational environment characterized by anxiety, uncertainty, and high demand for information;
3. a nexus of economic and trade uncertainty/ disruption, emergency procurement processes compounded by the wide availability of nefarious cyber tools.

In terms of the COVID-19-related cyber threat landscape, this report has found that cybercriminals and state-sponsored actors have both been very active in leveraging the pandemic. A surge in amateur and largely unsophisticated cyberattacks (e.g. phishing) was notably observed. Meanwhile, a plethora of professional cybercrime groups (e.g. *Maze, Doppelpaymer, Ryuk,* etc.) have also leveraged the pandemic and deployed ploys linked to the coronavirus. Moreover, state-sponsored cyber actors locked into ongoing rivalries or conflicts have also leveraged the pandemic to their ends. Some of them have also pursued pandemic-related strategic targets, such as health institutions or organizations in Wuhan.

The types of threats that exploited the pandemic are varied, with reports highlighting a spectrum ranging from large-scale and indiscriminate credential phishing, malspam, and scam campaigns to targeted spear-phishing, ransomware, DDoS or BEC attacks. Teleworking infrastructures, such as cloud based services, RDP connections or VPNs have also been subjects to intense attacks. Mobile threats, such as malware-loaded contact-tracing applications, have also been prevalent.

Targets have shown to be similarly diverse, with some of the most affected ones being individual users (including vulnerable groups like children, and the elderly), the public sector alongside certain critical infrastructure operators, especially healthcare and financial institutions. Following an opportunistic logic, the most affected countries have been those that were the most affected by the virus, such as Spain, Italy, the US, India, or Japan. As such, the cyberattacks have followed and adapted alongside the geographic spread of the virus.

The continuously dynamic nature of cyber threats is reflected in the transformation the landscape has undergone in response to the pandemic in the first six months of 2020. Among the numerous – mostly qualitative – changes in adversarial behavior, this report generally found that:

1. The coronavirus pandemic has forced a number of threat actors to adapt their criminal business model, particularly those in targeting sectors affected by restrictions or that required an in-person or physical element to their ploy.
2. The scale and sophistication of cyberattacks have increased, while certain actors have changed their *modus operandi*. This applies in particular to ransomware, where threat actors have increasingly resorted to double extortion methods and reduced encryption activation times in order to maximize their profit in an uncertain climate, an aggressiveness that is also reflected in DDoS attacks that have grown more intense.
3. The geographical distribution and types of targets have been opportunistic, targeting mainly those most affected and under pressure by the pandemic (e.g. the public, sector, the healthcare and education sector, or teleworking services), while shifting away (for now) from individuals and small businesses.
4. The first six months of the pandemic have expanded the motivations for state-sponsored actors to include coronavirus-related espionage (e.g. on vaccine research or infection rates) and targeting healthcare and critical research infrastructure. The extent to which this serves as a premise for the future will remain to be seen.

Despite these important changes, the cyber threat landscape of Q1 and Q2 shares many similarities with trends predating the pandemic. It is thus relatively continuous, both qualitatively and quantitatively, when referred to the dynamism, adaptability and types of attacks, the types of threat actors, or the overall volume of certain cyber threats. Most notably, despite general reporting of an unprecedented wave of phishing, COVID-19-related phishing and malspam represented only a small share of the overall volumes.

***

Overall, the cyber threat landscape of Q1 and Q2 2020 – operating under the above-mentioned special circumstances – is characterized by heightened risks and threats. The first wave of the pandemic has offered new opportunities for attacks, many of which relate specifically to the coronavirus while others have been leveraged for all types of attacks. The early months of the pandemic have also led to an expanded attack surface, thanks notably to the increasing digitization and its underlining use and dependence on digital infrastructure (e.g. cloud-based services, telework, etc.).

While some qualification of threat perspectives has set in following an initial rise of blanket concern, new infection waves, vaccine testing, and new rounds of financial aids provide ample opportunities for abuse. Even though some socio-technical factors might have evolved – or been less prevalent – since Q1 and Q2, their underlining driving forces have not. The climate will remain characterized by uncertainty, tension, and mistrust. Meanwhile, telework – and all its implications in terms of network security and cybersecurity – will also become more of the norm.

As such, this report aims to highlight three key recommendations in times of increased threat levels:

1. As economic pressure will become more structural and various cyber threats continue to mature and adapt, the importance of cybersecurity awareness-raising, capacity building, and communication with all stakeholders will be critical. Particular efforts should be made around authentications methods and basic cyber-hygiene, both of which could undermine the development and spread of credential phishing/stealing.
2. The importance of information exchange, cooperation, and coordination between all stakeholders cannot be sufficiently underlined. Such initiatives (e.g. round tables and bottom-up mobilization) are critical for fostering a better understanding and more comprehensive view of the evolving cyber threat landscape, bridging institutional gaps, and fostering trust. The various stakeholders should therefore aim at continuing and building upon these efforts in the future.
3. The accelerated digitization and adoption of telework has brought the issues of remote and cloud security to the forefront of cybersecurity. Besides all the security flaws and vulnerabilities linked to widely popular cloud-based applications – that need to be addressed by the responsible actors – users and companies, especially SMEs, need to start addressing the issues around the use of personal devices and the secure configuration of remote access technologies.

Bibliography

Abrams, L., 2020a. Ransomware Gangs to Stop Attacking Health Orgs During Pandemic. Bleeping Comput.

Abrams, L., 2020b. New CoronaVirus Ransomware Acts as Cover for Kpot Infostealer.

Abrams, L., 2020c. Netwalker Ransomware Infecting Users via Coronavirus Phishing. Bleepingcomputer.

Abrams, L., 2020d. Data-Stealing FormBook Malware Preys on Coronavirus Fears.

Abrams, L., 2020e. TrickBot Malware Targets Italy in Fake WHO Coronavirus Emails. Bleeping Comput.

Action Fraud, 2020a. Coronavirus-related fraud reports increase by 400% in March.

Action Fraud, 2020b. Public urged to flag coronavirus related email scams as online security campaign launches.

Afifi-Sabet, K., 2020. Hackers torn over how to adapt their tactics to the coronavirus pandemic.

Alfasi, S., 2020. COVID-19, Info Stealer & the Map of Threats – Threat Analysis Report. Reason Secur. URL https://blog.reasonsecurity.com/2020/03/09/covid-19-info-stealer-the-map-of-threats-threat-analysis-report/

Amnesty International, 2020. Contact Tracing App security flaw exposed sensitive personal details of more than one million. Amnesty Int. URL https://www.amnestyusa.org/press-releases/contact-tracing-app-security-flaw-exposed-sensitive-personal-details-of-more-than-one-million/

Anomali Threat Research Team, 2020. Anomali Threat Research Identifies Fake COVID-19 Contact Tracing Apps Used to Download Malware that Monitors Devices, Steals Personal Data. URL https://www.anomali.com/blog/anomali-threat-research-identifies-fake-covid-19-contact-tracing-apps-used-to-monitor-devices-steal-personal-data

Aprozper, A., 2020. 127% Increase in exposed RDPS due to surge in remote work. Reposify. URL https://blog.reposify.com/127-increase-in-exposed-rdps-due-to-surge-in-remote-work

Arampatzis, A., 2020. Cybersecurity World Dominated by the COVID-19 Pandemic. State Secur. URL https://www.tripwire.com/state-of-security/featured/covid-19-pandemic-dominates-cybersecurity-world/ (accessed 12.22.20).

Arsene, L., 2020a. 5 Times More Coronavirus-themed Malware Reports during March. Hot Secur. Bitdefender. URL https://labs.bitdefender.com/2020/03/5-times-more-coronavirus-themed-malware-reports-during-march/

Arsene, L., 2020b. New Router DNS Hijacking Attacks Abuse Bitbucket to Host Infosteale. Hot Secur. Bitdefender. URL https://labs.bitdefender.com/2020/03/new-router-dns-hijacking-attacks-abuse-bitbucket-to-host-infostealer/

Arsene, L., march. Coronavirus Medical Supply Scams Prey on Fear. Hot Secur. Bitdefender. URL https://hotforsecurity.bitdefender.com/blog/coronavirus-medical-supply-scams-prey-on-fear-22570.html

Arsene, L., march. Coronavirus Phishing Scams Exploit Misinformation. Hot Secur. Bitdefender. URL https://hotforsecurity.bitdefender.com/blog/coronavirus-phishing-scams-exploit-misinformation-22599.html

Asoltanei, O., Arsene, L., Mateescu, A., Barbatei, A.M., 2020. Android Apps and Malware Capitalize on Coronavirus. Bitdefender. URL https://labs.bitdefender.com/2020/03/android-apps-and-malware-capitalize-on-coronavirus/

Associated Press, 2020. In Pandemic, Rumors of Martial Law Fly Despite Reassurances.

Australian Government, 2020. Australia's Cyber Security Strategy 2020.

AWS Shield, 2020. AWS Shield: Threat Landscape Report – Q 1 2020.

Barth, B., 2020. U.S. universities at risk of back-to-school and Covid-19 email fraud. SC Mag.

Bing, C., Stubbs, J., Satter, R., 2020. Exclusive: Elite hackers target WHO as coronavirus cyberattacks spike. Reuters.

Bitcoin.org, 2018. Foire aux questions [WWW Document]. Bitcoin. URL https://bitcoin.org/fr/faq#qu-est-ce-que-bitcoin (accessed 2.14.18).

Blueliv, 2020. M00nD3v, HawkEye threat actor, sells malware after COVID-19 diagnosis. Blueliv. URL https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/covid-19-cybercrime-m00nd3v-hawkeye-malware-threat-actor/

Brumaghin, E., Unterbrink, H., 2020. New HawkEye Reborn Variant Emerges Following Ownership Change. Talos Blog. URL https://blog.talosintelligence.com/2019/04/hawkeye-reborn.html

Brunt, M., 29.30.20. Coronavirus: Fraud victims have lost more than £4.6m to virus-related scams. Sky News.

Burt, T., 2020. Microsoft report shows increasing sophistication of cyber threats. Microsoft. URL https://blogs.microsoft.com/on-the-issues/2020/09/29/microsoft-digital-defense-report-cyber-threats/

Bytagig, 2020. DDoS strikes explode as hackers exploit the global health crisis. Bytagig. URL https://www.bytagig.com/2020-sees-the-biggest-ddos-attack-during-covid-19-pandemic/

Canadian Center for Cybersecurity, 2020. Cyber Threat Bulletin: Impact of COVID-19 on Cyber Threat Activity. Cyber Threat Bull. URL https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-impact-covid-19-cyber-threat-activity

Canter, L., 2020. Coronavirus: Half of remote workers "victims of cybercrime." Yahoo.

Caroll, N., Sadowski, A., Laila, A., Hruska, V., Nixon, M., Ma, D., Haines, J., 2020. The Impact of COVID-19 on Health Behavior, Stress, Financial and Food Security among Middle to High Income Canadian Families with Young Children. Nutrients, 12.

Centre for Data Ethics and Innovation, 2019. Deepfakes and Audio-visual Disinformation, CDEI Snapshot Series. Centre for Data Ethics and Innovation.

CERT-MU, 2020. Cybercriminals Utilizing the Covid-19 Pandemic as a Cyberattack Vector.

Chebyshev, V., Sinitsyn, F., Parinov, D., Kupreev, O., Evgeny Lopatin, Kulaev, A., 2020. IT threat evolution Q1 2020. Statistics. SecureList. URL https://securelist.com/it-threat-evolution-q1-2020-statistics/96959/

Check Point Software Technologies, 2020a. Cyber Attack Trends: 2020 Mid-Year report.

Check Point Software Technologies, 2020b. COVID-19 Impact: Cyber Criminals Target Zoom Domains. Checkpoint. URL https://blog.checkpoint.com/2020/03/30/covid-19-impact-cyber-criminals-target-zoom-domains/

Check Point Software Technologies, 2020c. Coronavirus cyber-attacks update: beware of the phish. Checkpoint. URL https://blog.checkpoint.com/2020/05/12/coronavirus-cyber-attacks-update-beware-of-the-phish/

Check Point Software Technologies, 2020d. Coronavirus cyber-attacks update: beware of the phish. Checkpoint. URL https://blog.checkpoint.com/2020/05/12/coronavirus-cyber-attacks-update-beware-of-the-phish/

Chu, Z., Gianvecchio, S., Wang, H., Jajodia, S., 2012. Detecting Automation of Twitter Accounts: Are You a Human, Bot, or Cyborg? IEEE Trans. Dependable Secure Comput. 9, 811–824. https://doi.org/10.1109/TDSC.2012.75

Cimpanu, C., 2020a. Kaspersky: RDP brute-force attacks have gone up since start of COVID-19. ZDNet.

Cimpanu, C., 2020b. State-sponsored hackers are now using coronavirus lures to infect their targets. ZDNet.

Cimpanu, C., 2020c. Microsoft: Under 2% of all daily malspam uses COVID-19 lures. ZDNet.

Cimpanu, C., 2020d. DarkHotel hackers use VPN zero-day to breach Chinese government agencies. ZDNet.

Cimpanu, C., 2020e. Thousands of COVID-19 scam and malware sites are being created on a daily basis. ZDNet.

Cimpanu, C., 2020f. There's now COVID-19 malware that will wipe your PC and rewrite your MBR. ZDNet.

Cimpanu, C., 2020g. D-Link and Linksys routers hacked to point users to coronavirus-themed malware. ZDNet.

Clark, L., 2020. COVID-19 Complicates the US-China Cyber Threat Landscape. The Diplomat.

Coker, J., 2020. One in Three Not Worried About Cybersecurity Despite Rise in Threats. Infosecurity.

Collins, S., McCombie, S., 2012. Stuxnet: the emergence of a new cyber weapon and its implications. J. Polic. Intell. Count. Terror. 7, 80–91. https://doi.org/10.1080/18335330.2012.653198

Command Five Pty Ltd, 2011. Advanced Persistent Threats: A Decade in Review.

Council on Foreign Relations, n.d. Cyber operations tracker [WWW Document]. Counc. Foreign Relat. URL https://www.cfr.org/cyber-operations/

Coveware, 2020. Ransomware Payments Up 33% in Q1 2020 [WWW Document]. Coveware Ransomware Recovery First Responders. URL https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report (accessed 12.15.20).

Crisanto, J.C., Prenio, J., 2020. Financial crime in times of Covid-19 – AML and cyber resilience measures.

Culnane, C., Teague, V., 2020. Security analysis of the NHS COVID-19 App. State It. URL https://www.stateofit.com/UKContactTracing/

CyberPeace Institute, 2020. How the COVID-19 Infodemic Accelerates Cyberattacks. URL https://cyberpeaceinstitute.org/blog/2020-03-26-the-covid-19-infodemic-and-malicious-cyber-activities

Cybersecurity & Infrastructure Security Agency, National Cyber Security Centre, 2020. COVID-19 Exploited by Malicious Cyber Actors.

Cyfirma, 2020. Global Covid 10 Related phishing campaign by North Korean operatives Lazarus exposed by Cyfirma Researchers. Cyfirma. URL https://www.cyfirma.com/early-warning/global-covid-19-related-phishing-campaign-by-north-korean-operatives-lazarus-group-exposed-by-cyfirma-researchers/

Cyjax, 2020. COVID-19 Critical Infrastructure Cyber Threat Brief.

Dawson, M., Wright, J., Omar, M., 2016. Mobile Devices: The Case for Cyber Security Hardened Systems, in: Mobile Computing and Wireless Networks: Concepts, Methodologies, Tools, and Applications. pp. 1103–1123. https://doi.org/10.4018/978-1-4666-8751-6.ch047

Degrippo, S., 2020a. TA505 Malware Threat Insights. Proofpoint. URL https://www.proofpoint.com/us/blog/threat-insight/ta505-and-others-launch-new-coronavirus-campaigns-now-largest-collection-attack

Degrippo, S., 2020b. Attackers Use Fake HIV Test Results to Target Insurance, Healthcare, and Pharmaceutical Companies Globally. URL https://www.proofpoint.com/us/corporate-blog/post/attackers-use-fake-hiv-test-results-target-insurance-healthcare-and

DellSecureWorks, 2014. Advanced Threat Protection with Dell SecureWorks Security Services. Dell Inc.

Deloitte, 2020. Working from home during the coronavirus crisis is far less common among public authorities than in the private sector. Deloitte. URL https://www2.deloitte.com/ch/en/pages/public-sector/articles/working-from-home-during-coronavirus-less-common-among-public-authorities.html#

Desai, S., 2020. New Android App Offers Coronavirus Safety Mask But Delivers SMS Trojan. Zscaler. URL https://www.zscaler.com/blogs/research/new-android-app-offers-coronavirus-safety-mask-delivers-sms-trojan

DiResta, R., Miller, C., Molter, V., Pomfret, J., Tiffert, G., 2020. Telling China's Story: The Chinese Communist Party's Campaign to Shape Global Narratives.

Dobbins, R., Hummel, R., 2020. Measuring the Cruellest Month |. NETSCOUT. URL https://www.netscout.com/blog/asert/measuring-cruellest-month (accessed 12.18.20).

Ducklin, P., 2020. Watch out! Scummy scammers target home deliveries. Naked Secur. URL https://nakedsecurity.sophos.com/2020/03/26/watch-out-scummy-scammers-target-home-deliveries/

ECSO, 2020. COVID-19 CYBERSECURITY RESPONSE PACKAGE.

EGI CSIRT, 2020. Academic data centers abused for crypto currency mining. EGI CSIRT. URL https://csirt.egi.eu/academic-data-centers-abused-for-crypto-currency-mining/

Emmons, T., 2020. Largest ever recorded Packet per second-Based DDoS attack mitigated by Akamai. URL https://blogs.akamai.com/2020/06/largest-ever-recorded-packet-per-secondbased-ddos-attack-mitigated-by-akamai.html

European Union Agency for Network and Information Security, 2016. Review of Cyber Hygiene practices. European Union, Heraklion, Geece.

Europol, 2020a. Pandemic Profiteering how criminals exploit the COVID-19 crisis. Europol.

Europol, 2020b. Internet Organized Crime Threat Assesement 2020.

Europol, 2020c. HOW CRIMINALS PROFIT FROM THE COVID-19 PANDEMIC.

Europol, 2020d. Catching the Virus - cybercrime, disinformation and the Covid-19 pandemic.

F, A., Scholten, S., 2020. Coronavirus Threat Landscape Update. Proofpoint. URL https://www.proofpoint.com/us/threat-insight/post/coronavirus-threat-landscape-update

FATF, 2020. COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses. Paris, France.

FBI, 2020a. Online Extortion scams increasing during the covid-19 crisi. Public Serv. Announc. URL https://www.ic3.gov/media/2020/200420.aspx

FBI, 2020b. IMPLEMENTATION OF FRAUDULENT COVID-19 SHIPPING AND INSURANCE FEES BY CRIMINAL ACTORS. Public Serv. Announc. URL https://www.ic3.gov/media/2020/200611.aspx

FBI, CISA, 2020. People's Republic of China (PRC) Targeting of COVID-19 Research Organizations. Public Serv. Announc. URL https://www.cisa.gov/sites/default/files/publications/Joint_FBI-CISA_PSA_PRC_Targeting_of_COVID-19_Research_Organizations_S508C.pdf

FBI National Press Office, 2020. FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic [WWW Document]. URL https://www.fbi.gov/news/pressrel/press-releases/fbi-anticipates-rise-in-business-email-compromise-schemes-related-to-the-covid-19-pandemic

Fidler, D.P., 2020. Cybersecurity in the Time of COVID-19. Counc. Foreign Relat. URL https://www.cfr.org/blog/cybersecurity-time-covid-19

Financial Crimes Enforcement Network, 2020. The Financial Crimes Enforcement Network Provides Further Information to Financial Institutions in Response to the Coronavirus Disease 2019 (COVID-19) Pandemic. Financ. Crimes Enforc. Netw. URL

https://www.fincen.gov/news/news-releases/financial-crimes-enforcement-network-provides-further-information-financial

FireEye Inc., 2014. APT28: A window into Russia's cyber espionage operations? (Special Report). FireEye Inc., Milpitas, CA.

Franceschi-Bicchierai, L., 2020a. Interest in Zoom Zero-Day Hacks Is 'Sky-High' as Meetings Move Online. Motherboard.

Franceschi-Bicchierai, L., 2020b. Hackers Are Selling a Critical Zoom Zero-Day Exploit for $500,000. Motherboard.

Galov, D., 2020. Remote spring: the rise of RDP bruteforce attacks. SecureList. URL https://securelist.com/remote-spring-the-rise-of-rdp-bruteforce-attacks/96820/

Gandler, A., Kessem, L., 2020. Zeus Sphinx Trojan Awakens Amidst Coronavirus Spam Frenzy. Secur. Intell. URL https://securityintelligence.com/posts/zeus-sphinx-trojan-awakens-amidst-coronavirus-spam-frenzy/

Gatlan, S., 2020. Ancient Tortoise BEC Scammers Launch Coronavirus-Themed Attack. Bleeping Comput.

Ghernaouti-Hélie, S., 2013. Cyberpower: crime, conflict and security in cyberspace, 1. ed. ed, Forensic sciences. EPFL Press, Lausanne.

Glenza, J., 2020. Coronavirus: US says Russia behind disinformation campaign. The Guardian.

Goodes, G., 2020. Most Government-Sponsored COVID-19 Contact Tracing Apps Are Insecure and Risk Exposing Users' Privacy and Data. Guardsquare. URL https://www.guardsquare.com/en/blog/report-proliferation-covid-19-contact-tracing-apps-exposes-significant-security-risks

Gov UK, 2020. Funding boost to help healthcare suppliers improve cyber security. Coronavirus. URL https://www.gov.uk/government/news/funding-boost-to-help-healthcare-suppliers-improve-cyber-security

GreAT, 2020a. APT trends report Q1 2020. SecureList. URL https://securelist.com/apt-trends-report-q1-2020/96826/

GreAT, 2020b. APT trends report Q2 2020. SecureList. URL https://securelist.com/apt-trends-report-q2-2020/97937/

Guirakhoo, A., 2020a. COVID-19: Dark Web Reaction. Digit. Shad. URL https://www.digitalshadows.com/blog-and-research/covid-19-dark-web-reactions/

Guirakhoo, A., 2020b. How Cybercriminals Are Taking Advantage Of COVID-19: Scams, Fraud, And Misinformation. Digit. Shad. URL https://www.digitalshadows.com/blog-and-research/how-cybercriminals-are-taking-advantage-of-covid-19-scams-fraud-misinformation/

Hargittai, E., Nguyen, M.H., 2020. Comment les Suisses sont restés en contact pendant la crise du coronavirus. Swissinfo.

Harwell, D., 2020. Thousands of Zoom video calls left exposed on open Web. Wash. Post.

Hassold, C., 2020. Scattered Canary Cybercrime Ring Exploits the COVID-19 Pandemic with Fraudulent Unemployment and CARES Act Claims. Agari Email Secur. Blog. URL https://www.agari.com/email-security-blog/covid-19-unemployment-fraud-cares-act/

Hegelich, S., 2016. Invasion of the social bots.

Hope, A., 2020a. Report Says DDoS Attacks Increased by Over 500% Because of the COVID-19 Pandemic. CPO Mag.

Hope, A., 2020b. Ryuk Ransomware Still Targeting Hospitals During the Coronavirus Pandemic. CPO Mag.

Hu, Z., Lin, X., Kaming, A.C., Xu, H., 2020. Impact of the COVID-19 Epidemic on Lifestyle Behaviors and Their Association With Subjective Well-Being Among the General Population in Mainland China: Cross-Sectional Study. J. Med. Internet Res. 22.

Huntley, S., 2020. Findings on COVID-19 and online security threats. Google Updat. Threat Anal. Group. URL https://blog.google/technology/safety-security/threat-analysis-group/findings-covid-19-and-online-security-threats/

IBM, 2020. IBM Security Study Finds Employees New to Working from Home Pose Security Risk. IBM News Room. URL https://newsroom.ibm.com/2020-06-22-IBM-Security-Study-Finds-Employees-New-to-Working-from-Home-Pose-Security-Risk

iDefense, 2020. Cybersecurity Risks related to Covid-19.

Intel471, 2020. COVID-19 pandemic: Through the cybercriminal's eyes. URL https://blog.intel471.com/2020/04/30/covid-19-pandemic-through-the-cybercriminals-eyes/

Internet Corporation For Assigned Names and Numbers, 2016. Glossary [WWW Document]. ICANN. URL https://www.icann.org/resources/pages/glossary-2014-02-03-en#i (accessed 11.4.16).

Interpol, 2020a. Global Landscape on Covid-19 cyberthreat.

Interpol, 2020b. Cybercrime: Covid-19 impact.

Intsights, 2020. The Cyber Threat Impact of COVID-19 to Global Business. Intsight.

Joyce, S., 2020. Limited Shifts in the Cyber Threat Landscape Driven by COVID-19. FireEye Threat Res. URL https://www.fireeye.com/blog/threat-

research/2020/04/limited-shifts-in-cyber-threat-landscape-driven-by-covid-19.html

Kaspersky, 2020. Top 7 Mobile Security Threats in 2020. usa.kaspersky.com. URL https://usa.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store (accessed 12.22.20).

Kemp, S., 2020. DIGITAL 2020: JULY GLOBAL STATSHOT. DataReportal. URL https://datareportal.com/reports/digital-2020-july-global-statshot

Khan, N.A., Brohi, S.N., Zaman, N., 2020. Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic. TechRxiv.

Krebs, B., 2020a. How Cybercriminals are Weathering COVID-19. Krebs Secur. URL https://krebsonsecurity.com/2020/04/how-cybercriminals-are-weathering-covid-19/

Krebs, B., 2020b. U.S. Secret Service: "Massive Fraud" Against State Unemployment Insurance Programs. Krebs Secur. URL https://krebsonsecurity.com/2020/05/u-s-secret-service-massive-fraud-against-state-unemployment-insurance-programs/

Krebs, B., 2020c. Unproven Coronavirus Therapy Proves Cash Cow for Shadow Pharmacies. Krebs Secur. URL https://krebsonsecurity.com/2020/04/unproven-coronavirus-therapy-proves-cash-cow-for-shadow-pharmacies/

Krebs, B., 2020d. Live Coronavirus Map Used to Spread Malware. Krebs Secur. URL https://krebsonsecurity.com/2020/03/live-coronavirus-map-used-to-spread-malware/

Kumaran, N., Lugani, S., 2020. Protecting businesses against cyber threats during COVID-19 and beyond. Google Cloud. URL https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond

Kupreev, O., Badovskaya, E., Alexander Gutnikov, 2020. DDoS attacks in Q2 2020. SecureList. URL https://securelist.com/ddos-attacks-in-q2-2020/98077/

Lakshmanan, R., 2020. Nation-State Hackers Caught Hiding Espionage Activities Behind Crypto Miners [WWW Document]. URL https://thehackernews.com/2020/12/nation-state-hackers-caught-hiding.html (accessed 12.15.20).

Lefferts, R., 2020. Microsoft shares new threat intelligence, security guidance during global crisis. URL https://www.microsoft.com/security/blog/2020/04/08/microsoft-shares-new-threat-intelligence-security-guidance-during-global-crisis/

Liska, A., 2020a. Early Analysis of Ransomware Attacks on the Healthcare Industry. URL https://www.recordedfuture.com/healthcare-ransomware-attacks/

Liska, A., 2020b. Continued Rise in Ransomware Attacks Against Healthcare Providers. URL https://www.recordedfuture.com/healthcare-provider-ransomware-attacks/

Lord, N., 2015. What is Social Engineering? Defining and Avoiding Common Social Engineering Threats [WWW Document]. Digit. Guard. URL https://digitalguardian.com/blog/what-social-engineering-defining-and-avoiding-common-social-engineering-threats (accessed 10.13.17).

Lyons, K., 2020. Google saw more than 18 million daily malware and phishing emails related to COVID-19 last week. The Verge.

Malwarebytes Threat Intelligence, 2020. APTs and COVID-19: How advanced persistent threats use the coronavirus as a lure.

McAfee, 2020a. Cloud Adoption and Risk Report: Work from Home Edition.

McAfee, 2020b. McAfee Labs COVID-19 Threat Report.

McAfee, 2020c. COVID-19 related Maclious File Detections [WWW Document]. McAfee. URL https://www.mcafee.com/enterprise/en-us/lp/covid-19-dashboard.html

Mehrotra, K., Thomson, A., Sebenius, A., 2020. Cyber Risks Abound as Employees Shift From Offices to Homes. Bloomberg.

MELANI, 2020. Information Assurance Situation in Switzerland and Internationally Semi-annual report 2020/1. MELANI.

Microsoft, 2020. Microsoft Digital Defense Report.

Microsoft Azure, 2020. Update #2 on Microsoft cloud services continuity. Microsoft Azure. URL https://azure.microsoft.com/en-us/blog/update-2-on-microsoft-cloud-services-continuity/

Microsoft Threat Protection Intelligence Team, 2020. Exploiting a crisis: How cybercriminals behaved during the outbreak. URL https://www.microsoft.com/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-during-the-outbreak/

Miller, M., 2020. FBI sees spike in cyber crime reports during coronavirus pandemic. TheHill.

Montalbano, E., 2020. Spearphishing Campaign Exploits COVID-19 To Spread Lokibot Infostealer. Threatpost.

Moran, D., 2020. Android Malware takes advantage of Covid-19. Buguroo. URL https://www.buguroo.com/en/labs/android-malware-takes-advantage-of-covid-19

Mouton, F., de Coning, A., 2020. COVID-19: Impact on the Cyber Security Threat Landscape.

Mu-Hyun, C., 2020. South Korea sees rise in smishing with coronavirus misinformation. ZDNet.

Muncaster, P., 2020a. Ransomware: from Entry to Ransom in Under 45 Minutes. Infosecurity.

Muncaster, P., 2020b. #COVID19 Attacks Still Less Than 2% of Total Threats. Infosecurity.

Muncaster, P., 2020c. #COVID19 Tracing App Leaks User Data. Infosecurity.

Muncaster, P., 2020d. #COVID19 Drives Phishing Emails Up 667% in Under a Month. Infosecurity.

Muncaster, P., 2020e. Global DDoS Extorters Demand Ransom from Firms. Infosecurity.

Najarian, A., 2020. Business Email Compromise (BEC) Scams: COVID-19 Related Email Attacks Top Threat to Financial Services. Agari Email Secur. Blog. URL https://www.agari.com/email-security-blog/business-email-compromise-bec-scams-covid-19-financial-services/

National Cyber Security Centre, 2020a. UK and allies expose Russian attacks on coronavirus vaccine development. Natl. Cyber Secur. Cent. URL https://www.ncsc.gov.uk/news/uk-and-allies-expose-russian-attacks-on-coronavirus-vaccine-development

National Cyber Security Centre, 2020b. Cyber warning issued for key healthcare organisations in UK and USA. Natl. Cyber Secur. Cent. URL https://www.ncsc.gov.uk/news/warning-issued-uk-usa-healthcare-organisations

National Cyber Security Centre, 2018. Reckless campaign of cyber attacks by Russian military intelligence service exposed. Natl. Cyber Secur. Cent. URL https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed

National Cyber Security Centre, Communications Security Establishement, National Security Agency, 2020. Advisory: APT29 targets COVID-19 vaccine development.

Newman, L.H., 2020. The Worst Hacks and Breaches of 2020 So Far. Wired.

Nexusguard, 2020. Threat Report Distributed Denial of Service (DDoS) Q1 2020.

nixu, 2020. Something Old, Something new. The Covid-19 threat landscape is mostly about rebranding existing tricks. Nixu. URL https://www.nixu.com/blog/something-old-something-new-covid-19-threat-landscape-mostly-about-rebranding-existing-tricks

NJCCIC, 2020. Extortionists Claiming to be APT Groups Threaten DDoS Attacks. URL https://www.cyber.nj.gov/alerts-advisories/extortionists-claiming-to-be-apt-groups-threaten-ddos-attacks

Novetta, 2016. Operation Blockbuster: Unraveling the long thread of the Sony attack. Novetta, McLean,Virginia, USA.

O'Donnell, L., 2020. Compromised Zoom Credentials Swapped in Underground Forums. Threatpost.

OECD, 2020. Unemployment rate [WWW Document]. OECD. URL https://data.oecd.org/unemp/unemployment-rate.htm

O'Neill, P.H., 2020. Chinese hackers and others are exploiting coronavirus fears for cyber espionage. MIT Technol. Rev.

Osborne, C., 2020. Zeus Sphinx malware resurrects to abuse COVID-19 fears. ZDNet.

Paganini, P., 2020. Syria-linked APT group SEA targets Android users with COVID19 lures. Secur. Aff.

PCmag, 2016a. Definition of: payload [WWW Document]. PCmag. URL http://www.pcmag.com/encyclopedia/term/48909/payload (accessed 12.12.16).

PCmag, 2016b. Definition of: Remote Desktop Services [WWW Document]. PCmag. URL http://www.pcmag.com/encyclopedia/term/63149/remote-desktop-services (accessed 1.3.17).

PCmag, 2016c. Definition of: virtual private network [WWW Document]. PCmag. URL http://www.pcmag.com/encyclopedia/term/53942/virtual-private-network (accessed 4.25.17).

PCtools, 2016. What is a Script Kiddie? [WWW Document]. PCtools Symantec. URL http://www.pctools.com/security-news/script-kiddie/ (accessed 3.20.17).

Peterson, P., 2020. Business Email Compromise (BEC): Coronavirus a Costly New Strain of Email Attack. Agari Email Secur. Blog. URL https://www.agari.com/email-security-blog/business-email-compromise-bec-coronavirus-covid-19/

Photon Research Team, 2020. Coronavirus As A Double-Edged Sword For Cybercriminals: Desperation Or Opportunity? Digit. Shad. URL https://www.digitalshadows.com/blog-and-research/coronavirus-as-a-double-edged-sword-for-cybercriminals/

Photon Research team, 2020. Charitable Endeavors On Cybercriminal Forums. Digit. Shad. URL https://www.digitalshadows.com/blog-and-research/charitable-endeavors-on-cybercriminal-forums/

Pišot, S., Milovanović, I., Šimunič, B., Gentile, A., Bosnar, K., Prot, F., Bianco, A., Coco, G.L., Bartoluci, S., Katović, D., Bakalár, P., Slančová, T.K., Tlučáková, L., Casals, C., Feka, K., Christogianni, A., Drid, P., 2020. Maintaining everyday life praxis in the time of COVID-19 pandemic measures (ELP-COVID-19 survey). Eur. J. Public Health.

Platt, J., Reaves, J., Kremez, V., 2020. IcedID Botnet | The Iceman Goes Phishing for US Tax Returns.

Sentin. Labs. URL https://labs.sentinelone.com/icedid-botnet-the-iceman-goes-phishing-for-us-tax-returns/

Proofpoint, 2020. Threat Snapshot: Coronavirus-related Lure Examples Across the U.S., Spain, Portugal, and the Netherlands. Proofpoint. URL https://www.proofpoint.com/us/threat-insight/post/threat-snapshot-coronavirus-related-lures-comprise-more-80-percent-threat

Proofpoint Threat Research Team, 2020. Ready-made COVID-19 Themed Phishing Templates Copy Government Websites Worldwide.

PYMNTS, 2020. FTC: $145M In COVID-Related Scams Since Jan. PYMNTS.com. URL https://www.pymnts.com/news/security-and-risk/2020/ftc-reports-145m-in-covid-scams-since-january/ (accessed 12.15.20).

QinetiQ Ltd, 2014. Command & Control: Understanding, denying, detecting. QinetiQ Ltd.

Radoini, A., 2020. Cyber-crime during the COVID-19 Pandemic. United Nationa Interreg. Crim. Justice Res. Inst.

Radware, 2020. Radware Cybersecurity Alert - Global Ransom DDoS Campaign Targeting Finance, Travel and E-Commerce.

Ranger, S., 2020. Coronavirus: Hackers are now launching dozens of email scams each day. ZDNet.

Raywood, D., 2020. Global DDoS Attack Dismissed as T-Mobile Misconfiguration. Infosecurity.

Reuters, 2020a. Czechs warn of imminent, large-scale cyberattacks on hospitals.

Reuters, 2020b. Czech hospitals report cyberattacks day after national watchdog's warning. Reuters.

Richardson, E., Mahle, J., 2020. Cyberattacks on the rise during the Covid-19 pandemic. Cincinnati Bus. Cour.

Rouse, M., 2017a. computer exploit [WWW Document]. TechTarget. URL http://searchsecurity.techtarget.com/definition/exploit (accessed 2.20.18).

Rouse, M., 2017b. machine learning [WWW Document]. TechTarget. URL http://whatis.techtarget.com/definition/machine-learning (accessed 10.12.17).

Saengphaibul, V., 2020. Latest Global COVID-19/Coronavirus Spearphishing Campaign Drops Infostealer. Fortinet. URL https://www.fortinet.com/blog/threat-research/latest-global-covid-19-coronavirus-spearphishing-campaign-drops-infostealer

Sahel, T., Anderson, C., n.d. CovidLock Update: Deeper Analysis of Coronavirus Android Ransomware. URL https://www.domaintools.com/resources/blog/covidlock-update-coronavirus-ransomware

Samet, A., 2020. 2020 US SOCIAL MEDIA USAGE: How the Coronavirus is Changing Consumer Behavior. Bus. Insid.

Sara Coble, 2020. Fatal Hospital Hack Linked to Russia. Infosecurity.

Satter, R., Bing, C., Menn, J., Stubbs, J., 2020. Exclusive: Hackers linked to Iran target WHO staff emails during coronavirus - sources. Reuters.

Scammell, R., 2020. Coronavirus hackers face the wrath of the cybersecurity community. Verdict.

Schless, H., 2020. Global mobile phishing encounters surged by 37% amid shift to work-from-home. URL https://blog.lookout.com/global-mobile-phishing-encounters-surged-by-37-percent-amid-wfh-shift (accessed 12.18.20).

Schneier, B., Bourdeaux, M., 2020. How Hackers and Spies Could Sabotage the Coronavirus Fight. Foreign Policy.

Seals, T., 2020. Revamped HawkEye Keylogger Swoops in on Coronavirus Fears. Threatpost.

Sentonas, michael, 2020. Global Survey: The Cybersecurity Reality of the COVID-19 Remote Workforce. Crowdstrike Blog. URL https://www.crowdstrike.com/blog/global-survey-the-cybersecurity-reality-of-the-covid-19-remote-workforce/

Shcherbakova, T., 2020. Fake deliveries in an age of lockdown. Kaspersky Dly. URL https://www.kaspersky.com/blog/covid-fake-delivery-service-spam-phishing/35125/

Shcherbakova, T., Sidorina, T., Kulikova, T., 2020. Spam and phishing in Q1 2020. SecureList. URL https://securelist.com/spam-and-phishing-in-q1-2020/97091/

Shodan, 2020. Trends in Internet Exposure. Shodan. URL https://blog.shodan.io/trends-in-internet-exposure/

Siciliano, R., 2015. What is a Remote Administration Tool (RAT)? [WWW Document]. McAfee Blog. URL https://securingtomorrow.mcafee.com/consumer/identity-protection/what-is-rat/ (accessed 11.4.16).

SingCERT, 2020. Capitalising on COVID-19 Pandemic. SingCERT. URL https://www.csa.gov.sg/singcert/publications/capitalising-on-covid19-pandemic

Smithers, R., 2020. Fraudsters use bogus NHS contact-tracing app in phishing scam. The Guardian.

Soguel, D., 2020. Switzerland sees more online crime amid coronavirus shock. Swissinfo.

Srikanth, R., 2017. DNS Hijacking: What is it and How it Works [WWW Document]. GoHacking. URL https://www.gohacking.com/dns-hijacking/ (accessed 3.2.17).

Städeli, M., 2020. Mit der Krise kam die Cyber-Angriffswelle: Die Attacken haben sich verdreifacht. NZZ Am Sonntag.

Starks, T., 2020. Early Covid-19 tracking apps easy prey for hackers, and it might get worse before it gets better. Politico.

Stefanko, L., 2020. New ransomware posing as COVID-19 tracing app targets Canada; ESET offers decryptor. WeliveSecurity. URL https://www.welivesecurity.com/2020/06/24/new-ransomware-uses-covid19-tracing-guise-target-canada-eset-decryptor/

Stein, S., Jacobs, J., 2020. Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak. Bloomberg.

Stolton, S., 2020. Von der Leyen: Chinese cyberattacks on EU hospitals 'can't be tolerated.' Euractiv.

Stone, J., 2020a. A Chinese security firm says DarkHotel hackers are behind an espionage campaign, but researchers want more details. Cyberscoop.

Stone, J., 2020b. Hackers use fake contact tracing apps in attempt to install banking malware on Android phones.

Stubbs, J., Bing, C., n.d. Exclusive: Iran-linked hackers recently targeted coronavirus drugmaker Gilead - sources. Reuters 08.05.2020.

Symantec, 2020. Threat Landscape Trends – Q1 2020. Symantec. URL https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/threat-landscape-q1-2020

Symantec Corporation, 2002. Trojan.Dropper [WWW Document]. Symantec. URL https://www.symantec.com/security_response/writeup.jsp?docid=2002-082718-3007-99 (accessed 12.8.16).

Szocs, E., Bejean, C., 2020. Malspam in the Time of COVID-19. Crowdstrike Blog. URL https://www.crowdstrike.com/blog/covid19-and-malspam/

TechTerms, 2016. IDS [WWW Document]. TechTerms. URL http://techterms.com/definition/ids (accessed 12.8.16).

Thaware, V., 2020a. COVID-19 Outbreak Prompts Opportunistic Wave of Malicious Email Campaigns. Symantec. URL https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/covid-19-outbreak-prompts-opportunistic-wave-malicious-email-campaigns

Thaware, V., 2020b. Text-Based COVID-19 Spam Wants Your Information, Money. Symantec. URL https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/covid-19-text-scam

The Economist, 2020. Covid nostra: The pandemic is creating fresh opportunities for organised crime. The Economist.

Threat intelligence team, 2020. APT36 jumps on the coronavirus bandwagon, delivers Crimson RAT. MalwareBytes Labs. URL https://blog.malwarebytes.com/threat-analysis/2020/03/apt36-jumps-on-the-coronavirus-bandwagon-delivers-crimson-rat/

Threat Intelligence Team, 2020. Fake "Corona Antivirus" distributes BlackNET remote administration tool. MalwareBytes Labs. URL https://blog.malwarebytes.com/threat-analysis/2020/03/fake-corona-antivirus-distributes-blacknet-remote-administration-tool/

Trend Micro, 2020a. Developing Story: COVID-19 Used in Malicious Campaigns. Trend Micro. URL https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

Trend Micro, 2020b. Emotet Uses Coronavirus Scare in Latest Campaign, Targets Japan. Trend Micro. URL https://www.trendmicro.com/vinfo/mx/security/news/cybercrime-and-digital-threats/emotet-uses-coronavirus-scare-in-latest-campaign-targets-japan

Trend Micro, 2020c. Lemon Duck Cryptominer Spreads through Covid-19 Themed Emails. Trend Micro. URL https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/lemon-duck-cryptominer-spreads-through-covid-19-themed-emails

Trend Micro, 2017. Ransomware [WWW Document]. Trend Micro. URL https://www.trendmicro.com/vinfo/us/security/definition/ransomware (accessed 2.19.18).

Trend Micro, n.d. Info stealer [WWW Document]. Trend Micro. URL https://www.trendmicro.com/vinfo/us/security/definition/Info-stealer

TrendMicro, 2017. Definition [WWW Document]. TrendMicro. URL http://www.trendmicro.com/vinfo/us/security/definition/data-breach (accessed 1.17.17).

Twingate, 2020. Cybersecurity in the Age of Coronavirus. Twingate. URL https://www.twingate.com/research/cybersecurity-in-the-age-of-coronavirus/

UK Finance, 2020. Fraud - The Fact 2020.

UNCTAD, 2020. Global Trade Update: COVID-19 causes international trade collapse.

UNICEF, 2020. COVID-19 and its implications for protecting children online.

Upatham, P., Treinen, J., 2020. Amid COVID-19, Global Orgs See a 148% Spike in Ransomware Attacks; Finance Industry Heavily Targeted. Vm Ware Carbon Black. URL https://www.carbonblack.com/blog/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted/

US Bureau of Labor Statistics, 2020. The employement situation - augsut 2020.
US Department of Defense, 2017. DOD Dictionary of Military and Associated Terms.
US District Court Western District of Pennsylvania, 2018. Case 2:18-cr-00263-MRH.
Vifian, P., Kaelin, A.W., Suter, M., Peter, M.K., Wettstein, N., 2020. Home office surge in Swiss SMEs: Opportunities taken – cyberrisks underestimated. gfs-Zurich.
Walter, J., 2020. Threat Intel | Cyber Attacks Leveraging the COVID-19/CoronaVirus Pandemic. Sentin. Labs. URL https://labs.sentinelone.com/threat-intel-update-cyber-attacks-leveraging-the-covid-19-coronavirus-pandemic/
Whitney, L., 2020. Cybercriminals now using malware and adware to exploit virtual meeting apps. TechRepublic.
WHO, 2020a. WHO reports fivefold increase in cyber attacks, urges vigilance.
WHO, 2020b. Beware of criminals pretending to be WHO.
Wiggen, J., 2020. The impact of COVID-19 on cyber crime and state-sponsored cyber activities.
Winder, D., 2020. Hackers Promise “No More Healthcare Cyber Attacks” During COVID-19 Crisis. Forbes.
Winder, D., 2019. 28 Million Android Phones Exposed To “Eye-Opening” Attack Risk. Forbes.
Yoachimik, O., Singh, A., 2020. Network-Layer DDoS Attack Trends for Q1 2020 [WWW Document]. Cloudflare Blog. URL https://blog.cloudflare.com/network-layer-ddos-attack-trends-for-q1-2020/ (accessed 12.18.20).
Zaboeva, C., 2020. German Task Force for COVID-19 Medical Equipment Targeted in Ongoing Phishing Campaign. Secur. Intell. URL https://securityintelligence.com/posts/german-task-force-for-covid-19-medical-equipment-targeted-in-ongoing-phishing-campaign/
Zurich, 2020. Fraud on the rise due to Coronavirus [WWW Document]. Zurich. URL https://www.zurich.co.uk/insurance/coronavirus/coronavirus-scams
Zurier, S., 2020. Rise in DDoS attacks lost in pandemic. SC Mag.

Annexes

Annex 1: Abbreviations

APT	Advanced Persistent Threat
BEC	Business Email Compromise
C&C	Command and Control
CDC	Center for Disease Control and Prevention
CSE	Communication Security Establishment Canada
DDoS	Distributed Denial of Service
CIO	Cyber-enabled Influence Operation
DNS	Domain Name System
DMARC	Domain-based Message Authentication, Reporting & Conformance
ECSO	European Cyber Security Organisation
ENISA	European Union Agency for Cybersecurity
FOPH	Federal Office of Public Health of the Swiss Confederation
GRU	Main Directorate of the General Staff of the Armed Forces of the Russian Federation
ISP	Internet Service Provider
ITU	International Telecommunication Union
NCSC	UK National Cybersecurity Center
NSA	US National Security Agency
RAT	Remote Access Trojan
RDP	Remote Desktop Protocol
SME	Small and Medium Enterprises
WHO	World Health Organization
VPN	Virtual Private Network

Annex 2: Glossary

Advanced Persistent Threat (APT): A threat that targets critical objectives to gain access to a computer system. Once inside a network, it tries to remain hidden and is usually difficult to remove when discovered (Command Five Pty Ltd, 2011; DellSecureWorks, 2014)

Bitcoin: Cryptocurrency and digital payment system working on the peer to peer system and without any central institution (Bitcoin.org, 2018)

Botnet or bot: Network of infected computers which can be accessed remotely and controlled centrally in order to launch coordinated attacks (Ghernaouti-Hélie, 2013, p. 427).

Command and Control (C2): "The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission" (US Department of Defense, 2017, p. 43).

Command and Control infrastructure (C&C): A server through which the person controlling malware communicates with it in order to send commands and retrieve data (QinetiQ Ltd, 2014, p. 2).

Cyber hygiene: Analogy to personal hygiene with regard to one's security and practices in cyberspace in order to protect networks and personal computers (European Union Agency for Network and Information Security, 2016).

Data breach: Event in which information of a sensitive nature is stolen from a network without the users' knowledge (TrendMicro, 2017).

Deepfake: A Video or audio file modified in which a person, object or environment is changed with the help of advanced software (Centre for Data Ethics and Innovation, 2019).

Distributed Denial of Service (DDoS): The act of overwhelming a system with a large number of packets through the simultaneous use of infected computers (Ghernaouti-Hélie, 2013, p. 431).

Domain Name Service (DNS): The address structure that translates Internet Protocol addresses into a string of letters that is easier to remember and use (Internet Corporation For Assigned Names and Numbers, 2016).

Domain Name Service (DNS) hijacking: A form of website defacement also referred to as DNS redirection, where a malicious attacker obtains unauthorized access to victims' computers and changes their DNS settings to another DNS server, which redirects victims to malicious websites (Srikanth, 2017).

Dropper: Element to disguise a malware into a legitimate application or file (Symantec Corporation, 2002).

Exploit: An attack on a computer operating system using a vulnerability of the system or software (Rouse, 2017a).

Hack: Act of entering a system without authorization (Ghernaouti-Hélie, 2013, p. 433).

Intrusion Detection System (IDS): A system used to observe for malicious traffic on a computer network (TechTerms, 2016)

Keylogger: Feature that traces keystrokes without the knowledge of the user (Novetta, 2016, p. 56).

Machine learning: An artificial intelligence that can learn from the data it receives and predict outcomes without the need to be reprogrammed (Rouse, 2017b).

Malware: Malicious software that can take the form of a virus, a worm or a Trojan horse (Collins and McCombie, 2012, p. 81).

Malware family: A collection of malware that share a significant amount of code (FireEye Inc., 2014, p. 21).

Master Boot Record (MBR): Information stored on the first sector of the hard disc, identifying the location of the system to load it in the main storage (Novetta, 2016, p. 56).

Patch: Software update that repairs one or several identified vulnerabilities (Ghernaouti-Hélie, 2013, p. 437).

Payload: The part of malware that causes harmful results (PCmag, 2016a).

Ransomware: Malware that locks the user's computer system and only unlocks it when a ransom is paid (Trend Micro, 2017).

Remote Administration or Access Tool (RAT): Software granting remote access and control to a computer without having physical access to it. RAT can be legitimate software, but also malicious (Siciliano, 2015).

Remote Desktop Protocol (RDP): A Microsoft's protocol to be able to access another computer's desktop (PCmag, 2016b).

Script kiddies: Attackers who use cybertools that have been developed by more experienced and sophisticated hackers. Their main motive is to gain attention (PCtools, 2016).

Social bots: Bot is a shorter term for robot. It is an automated program that runs routine tasks on social media but can also define fake social media accounts that are used to repost messages or news and/or to spam (Chu et al., 2012; Hegelich, 2016).

Social engineering: a non-technical strategy cyber attackers use that relies heavily on human interaction and often involves tricking people into breaking standard security practices (Lord, 2015).

Spamming: Messages, comments or posts sent in large quantities via email or on social media (Ghernaouti-Hélie, 2013, p. 440).

Spear-phishing: A sophisticated phishing technique that not only imitates legitimate webpages, but also selects potential targets and adapts malicious emails to them. Emails often look like they come from a colleague or a legitimate company (Ghernaouti-Hélie, 2013, p. 440).

Spoofing: Act of usurping IP addresses in order to commit malicious acts such as breaching a network (Ghernaouti-Hélie, 2013, p. 440).

Trojan horse: Malware hidden in a legitimate program in order to infect and hijack a system (Ghernaouti-Hélie, 2013, p. 441).

Virus: Malicious program with the capacity to multiply itself and to impair an infected system. Its purpose is also to spread to other networks (Ghernaouti-Hélie, 2013, p. 442).

Virtual Private Network (VPN): Private network within a public network that uses encryption to remain private (PCmag, 2016c).

Wiper: Feature that completely erases data from a hard disk (Novetta, 2016, p. 57).